EIGENSPACES AND THE TAME KERNEL

Aimée Herczog

Eigenspaces and the tame kernel

Eigenspaces and the tame kernel

Een wetenschappelijke proeve op het gebied van de
Wiskunde en Informatica

PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Katholieke Universiteit Nijmegen,
volgens het besluit van het College van Decanen, in het
openbaar te verdedigen op woensdag 14 mei 1997
des namiddags om 1.30 uur precies
door

Aimée Herczog

geboren op 17 december 1966
te Amsterdam

Promotor: Prof. Dr. A.H.M. Levelt
Co-promotor: Dr. F.J. Keune

Leden van de manuscriptcommissie:
Dr. J. Brinkhuis (Erasmus Universiteit Rotterdam)
Prof. Dr. J. Browkin (University of Warsaw)

ISBN 90-9010373-2

Contents

Introduction

This thesis consists of three chapters. The connection between these chapters is the isomorphism

$$(Cl(O_{F(\zeta_p)})/p)_{\omega^{-1}} \cong K_2O_F/p.$$

Here F is an Abelian number field, O_F is the ring of integers of F, and p is an odd prime, which is unramified in F and does not divide the degree $[F : \mathbf{Q}]$. For the proof of this isomorphism we need the exact sequence

$$0 \to (\mu_p \otimes Cl(O_{F(\zeta_p)}[\tfrac{1}{p}]))^{\Gamma} \to K_2O_F/p \to \bigoplus_{p \in S'} \mu_p \to 0$$

of Keune (see [K]).

In chapter 1 and 2 we will take a closer look at the left side of the isomorphism. For this purpose is

$$(O \otimes_{\mathbf{Z}_p} Cl(O_{F(\zeta_p)})/p)_{\omega^{-1}}$$

rewritten as

$$(\bigoplus_{\chi \text{ odd}} (O \otimes_{\mathbf{Z}_p} Cl(O_{F(\zeta_p)})/p)_{\omega^{-1}\chi}) \bigoplus (\bigoplus_{\chi \text{ even}} (O \otimes_{\mathbf{Z}_p} Cl(O_{F(\zeta_p)})/p)_{\omega^{-1}\chi}),$$

where O is a ring extension of $\mathbf{Z}_p$ generated by the values of the characters in the character group of $\mathrm{Gal}(F/\mathbf{Q})$.

In chapter 1, the numbers of elements of the odd part are expressed as Bernoulli numbers. In chapter 2, the numbers of elements of the even part are expressed as numbers of elements of eigenspaces of the global units modulo the cyclotomic units. In chapter 3, the vested results of chapter 1 and 2 are applied to the right side of the isomorphism, in order to investigate the structure of the tame kernel.

The size of the eigenspaces of the ideal class group has been examined by others. For example, Mazur and Wiles ([M-W]) proved for the odd components of an ideal class group:

Theorem 0.1 *Let F be an Abelian imaginary field extension of $\mathbf{Q}$ of degree prime to p, write $A(F)$ for its ideal class group and let χ: $Gal(F/\mathbf{Q}) \to O^*$ be a p-adic odd character of order prime to p. Then the order of $A(F)^\chi$ has the same p-adic valuation as $B_1(\chi^{-1})^g$ where $g = [O : \mathbf{Z}_p]$.*

For the even components Greither ([Gr]) proved:

Theorem 0.2 *Let $F/\mathbf{Q}$ be real with Galois group G. Suppose the p-part G_p of G is cyclic. Write $G = G_0 \times G_p$. Let E be the group of units of F and let C_F be the group of circular units of F in the sense of Sinott, $C = C_F \cap E$. Then we have for all nontrivial characters χ of G_0*

$$|(E/C)_\chi| = |A(F)_\chi| 2^h |(R : U)_\chi|,$$

where $R = \mathbf{Z}[G]$ and U are as in Sinott ([Si2]).

Note that if the p-part of G is cyclic, then p does not divide $(R : U)$ (see [Si2]).

Using Euler systems in the way it is done by Rubin gives us in chapter 1 an if and only if relation for an odd component of the ideal class group to be cyclic. Unfortunately the primes needed for computations are too large, but I think it is interesting in its own right.
For the application of the theorems of Rubin we need in chapter 2 an explicit generator of the eigenspace of the global units modulo the cyclotomic units. This has the advantage that computations can be made as performed in chapter 3.
In chapter 3 the structure of the p-rank of the tame kernel of several real quadratic number fields will be computed, where p is an odd prime. It turns out that for all real quadratic fields F with discriminant less then 20000, the p-rank of the tame kernel is always cyclic except for a few cases which I am unable to compute. Recently Browkin pointed out to

me that for $p = 5$ the p-rank of the tame kernel of a real quadratic number field does not always have to be cyclic. A possible counterexample, based on work by Mestre ([Mes]), will be given.
For the real cyclotomic field a list with structures of the tame kernel is given. This is done to show that the theory in chapter 3 works for any Abelian field subject to some conditions. It turns out that in some cases the structure of the ideal class group can be determined by knowledge of the structure of the tame kernel. So the isomorphism works in both ways. In most cases, however, the structure of the ideal class group is necessary to determine the structure of the tame kernel through the above isomorphism.

Chapter 1

Odd characters and the ideal class group

1.1 Introduction

Kolyvagin introduced in [Ko] a general system, the so-called Euler system, which he applied amongst others to Gauss sums and to cyclotomic units. In this way he was able to determine the orders of the different eigenspaces of the ideal class group of $\mathbf{Q}(\zeta_p)$. Rubin simplified and genereralized the ideas of Kolyvagin. In this chapter I will give an outline of Rubin's proof. It is shown that his proof can be extended to an arbitrary Abelian field subject to some conditions. To be more precise, if K is an Abelian number field and $K \subset \mathbf{Q}(\zeta_{\mathrm{cond}(K)})$ with $p \nmid \phi(\mathrm{cond}(K))$, then the number of elements of an odd χ component of the ideal class group equals the p-part of a Bernoulli number. The possibility of such an extension was already mentioned in [Ru2]. In a more general setting, namely for F an Abelian imaginary field extension of $\mathbf{Q}$ of degree prime to p, Mazur and Wiles proved this using Iwasawa theory (see [M-W]). However, the proof of Rubin is much simpler. The odd χ components of the ideal class group are examined using Gauss sums. The minus class groups can also be analyzed using the units as Euler systems and

Kummer duality (see [Ru1]).

1.2 Preliminaries

In this section I give an overview of concepts which are frequently used, but first I will explain what an Euler system is. An Euler system can be thought of as a collection of points of some algebraic group, related by two conditions, namely a norm property and a congruence property. Rubin showed that for a number of applications this congruence property can be removed. For this he introduced the "universal Euler system", which is defined as follows (see [Ru3]).

Definition 1.1 *Let $F/\mathbf{Q}$ be Abelian and let S be the set of positive squarefree integers which are only divisible by primes l which split completely in F and in $\mathbf{Q}(\zeta_M)$ with M a power of a fixed odd prime p. Suppose $n \in S$ then $\{x(n) : n \in S\}$ forms an* Euler system *for F if it satisfies i) and ii) respectively iii).*

i). $x(n) \in F(\zeta_n)^*$,

ii). $N_l x(n) \equiv (Fr_l - 1)x(\frac{n}{l})$ *mod* $F(\zeta_{n/l})^{*^M}$,

iii). $N_l x(n) \equiv (1 - Fr_l^{-1})x(\frac{n}{l})$ *mod* $F(\zeta_{n/l})^{*^M}$.

Properties (ii) and (iii) are not essentially different. For example, the cyclotomic units form an Euler system satisfying (ii) or (iii). It depends on the choice of the units which one is preferable. We will see later that the Euler system of Gauss sums as in [Ru2] satifies (i) and (iii), and the Euler system of cyclotomic units as in [Ru1] satisfies (i) and (ii).

1.2.1 Group representations and characters

Definition 1.2 *Let F be a field and G a finite group. Then an* F-representation *of G is a homomorphism $\Xi : G \to GL(n, F)$ for some integer n. The* character χ *of G afforded by Ξ is the function given by $\chi(g) = tr\ \Xi(g)$.*

Representations are a different way of looking at modules. If A is an F-algebra, then there is a one-to-one correspondence between isomorphism classes of A-modules and similarity classes of representations of A. Two representations Ξ and Ψ of degree n are similar if there exists a nonsingular $n \times n$ matrix P over F, such that $\Xi(a) = P^{-1}\Psi(a)P$ for all $a \in A$.

We have the following properties:

i). If χ is the character afforded by Ξ then $n = \dim \Xi = \chi(1)$. If $n = 1$ then χ is called a linear character,

ii). Let Ξ and Ψ afford characters χ and ψ, then the character $\chi\psi$ of G is given by $\chi\psi(g) = \text{tr}\,(\Xi(g) \otimes \Psi(g))$. The notation $\Xi \otimes \Psi$ will also be used,

iii). A representation is irreducible if the corresponding module is irreducible,

iv). If $N \triangleleft G$ and $N \subseteq \ker \Xi$, then there is a unique F -representation $\bar{\Xi}$ of G/N defined by $\bar{\Xi}(Ng) = \Xi(g)$. Conversely, if $\bar{\Xi}$ is given, we can define a representation Ξ on G by $\Xi(g) = \bar{\Xi}(Ng)$,

v). Ξ is irreducible $\Leftrightarrow \bar{\Xi}$ is irreducible,

vi). Suppose $G = H \times K$. Let ϕ be a character of H and let ψ be a character of K. Using (iv) we see that under the isomorphism $H \cong G/K$ there is a corresponding character $\hat{\phi}$ of G with $K \subseteq \ker \hat{\phi}$ and $\hat{\phi}(hk) = \phi(h)$. In a similar way we can define a character $\hat{\psi}$ on G. It follows that $\phi \times \psi = \hat{\phi}\hat{\psi}$ is a character of G,

vii). If $G = H \times K$ then the irreducible characters of G are the characters $\phi \times \psi$ where ϕ and ψ are the irreducible characters of H and K,

viii). The algebraic closure $\bar{F}$ of F is a splitting field for G. This means for G Abelian, that Ξ regarded as a $\bar{F}$ -representation is a diagonal matrix with entries irreducible representations of dimension 1.

This is denoted by $\Xi = \sum \rho_i$. I will make no distinction between the linear characters and the one dimensional representations. Note that if we adjoin the values of the entries to F we also obtain a splitting field,

ix). The contragradient $\hat{\Xi}$ is a homomorphism $\hat{\Xi} : G \to GL(n, F)$ given by $\hat{\Xi}(g) =^T \Xi(g^{-1})$, where T denotes "transpose".

For more on this topic and proofs see [I].

Dirichlet characters

If we take $F = \mathbf{C}$ and $G = (\mathbf{Z}/n\mathbf{Z})^*$, then the character χ afforded by a one dimensional representation is called a Dirichlet character. Through a fixed isomorphism $\mathbf{C} \cong \mathbf{C}_p$, we consider Dirichlet characters as p-adic characters. Suppose $n \mid m$, then we have a homomorphism from $(\mathbf{Z}/m\mathbf{Z})^*$ to $\mathbf{C}$ by composing. This induces a character mod m.

Definition 1.3 *A character χ is called* primitive *if it cannot be induced by a character mod n for any divisor n of m with $n \neq m$. In that case m is called the* conductor f_χ *of χ.*

In this thesis all the characters are assumed to be primitive. If we write about the characters of $(\mathbf{Z}/n\mathbf{Z})^*$, we include characters of conductor dividing n. Let χ and ψ be Dirichlet characters of conductors f_χ, f_ψ. Then $\chi\psi$ is defined as the primitive character associated to γ, where γ is the homomorphism

$$\gamma : (\mathbf{Z}/\mathrm{lcm}(f_\chi, f_\psi)\mathbf{Z})^* \to \mathbf{C}^*$$

defined by $\gamma(a) = \chi(a)\psi(a)$. We will most of the time consider Dirichlet characters as characters of Galois groups of cyclotomic fields, through the isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^*$. The set of all primitive Dirichlet characters forms an Abelian group, called the character group of G, and is denoted by $\hat{G}$.

We have the following properties:

i). We can extend χ to $\mathbf{Z}$ by letting $\chi(a) = 0$ if $(a, f_\chi) \neq 1$,

ii). If $(f_\chi, f_\psi) = 1$ then $f_{\chi\psi} = f_\chi f_\psi$,

iii). $\chi(a)\psi(a) = \chi\psi(a)$ unless $\chi(a) = \psi(a) = 0$ for arbitrary χ and ψ,

iv). χ is called even if $\chi(-1) = 1$ and odd if $\chi(-1) = -1$,

v). If we take $n = p$ there exists a unique character ω such that $\omega(a) \equiv a \bmod p$ for all integers a, with $p \nmid a$. This character is called the Teichmüller character.

1.2.2 Gauss sums

Definition 1.4 *Let r be a prime and $\chi : (\mathbf{Z}/r\mathbf{Z})^* \to \mathbf{C}$ a Dirichlet character. Fix a primitive r-th root of unity ζ_r, then the* Gauss sum *is defined by*

$$\tau(\chi) = \sum_{a \in (\mathbf{Z}/r\mathbf{Z})^*} \chi(a)\zeta_r^a.$$

We have the following properties:

i). If the order of χ is m then $\tau(\chi) \in \mathbf{Q}(\zeta_{mr})$,

ii). If $\chi \neq 1$, then $\tau(\chi)\tau(\bar{\chi}) = \chi(-1)r$,

iii). If $\sigma_b \in \mathrm{Gal}(\mathbf{Q}(\zeta_r, \zeta_m)/\mathbf{Q}(\zeta_r))$ such that $\sigma_b : \zeta_m \to \zeta_m^b$ then $\tau(\chi)^{\sigma_b} = \tau(\chi^b)$,

iv). If $\sigma_c \in \mathrm{Gal}(\mathbf{Q}(\zeta_r, \zeta_m)/\mathbf{Q}(\zeta_m))$ such that $\sigma_c : \zeta_r \to \zeta_r^c$ then $\tau(\chi)^{\sigma_c} = \chi(c)^{-1}\tau(\chi)$,

v). If $r \equiv 1 \bmod l$ then $\prod_{\psi^l=1} \tau(\psi\chi) = -\tau(\chi^l)\chi(l^{-l}) \prod_{\psi^l=1} \tau(\psi)$.

Property (v) is known as the Davenport-Hasse distribution relation (see [La2]). Now we will determine the prime factorization of the Gauss sum

(see [La1],[La2]). Let r be a prime and let $\mathfrak{r}$ be a prime ideal of $\mathbf{Q}(\zeta_{r-1})$ above r. Since $\mathbf{Z}[\zeta_{r-1}]$ mod $\mathfrak{r}$ is the finite field with r elements and since the $(r-1)$-st roots of unity are distinct mod $\mathfrak{r}$, there is an isomorphism

$$v = v_{\mathfrak{r}} : \mathbf{F}_r^* \to \mu_{r-1} \subseteq \mathbf{Q}(\zeta_{r-1}),$$

defined by

$$v(a) = \zeta_{r-1}^k, \text{ such that } \zeta_{r-1}^k \equiv a \bmod \mathfrak{r}.$$

Next we lift this v to a Dirichlet character

$$v : \mathbf{Z} \to \mu_{r-1} \cup \{0\}.$$

This Dirichlet character generates the character group of $\mathbf{F}_r^*$, so every character χ of the character group of $\mathbf{F}_r^*$ is an integral power of v. Let k be any integer $0 \leq k \leq r-2$ and $\mathfrak{R}$ a prime ideal lying above $\mathfrak{r}$ in $\mathbf{Q}(\zeta_{r-1}, \zeta_r)$. Then we have the congruence

$$\frac{\tau(v^{-k})}{(\zeta_r - 1)^k} \equiv \frac{-1}{k!} \bmod \mathfrak{R}.$$

This gives us the order of the Gauss sum at one prime above r.

Lemma 1.1 *Let m be an integer, such that $m \mid r-1$, and $\mathfrak{r}$ a prime ideal lying above r in $\mathbf{Q}(\zeta_m)$ and $\mathfrak{R}$ a prime ideal lying above $\mathfrak{r}$ in $\mathbf{Q}(\zeta_m, \zeta_r)$. Let v be the dirichlet character as defined above, take $k = \frac{r-1}{m}$ and write $s(k, \mathfrak{r}) = \frac{1}{m} \sum_{c \in (\mathbf{Z}/m\mathbf{Z})^*} c\sigma_c^{-1}$, then we have the ideal factorization*

$$(\tau(v^{-k})) = \mathfrak{R}^{(r-1)s(k,\mathfrak{r})}.$$

Proof. We obtain from the congruence $\mathrm{ord}_{\mathfrak{R}}\tau(v^{-k}) = k$, since $\zeta_r - 1$ is a prime element of $\mathbf{Q}(\zeta_r)$ and it remains unramified in $\mathbf{Q}(\zeta_m, \zeta_r)$. Also

$$\begin{aligned} \mathrm{ord}_{\sigma_c^{-1}\mathfrak{R}}\tau(v^{-k}) &= \mathrm{ord}_{\mathfrak{R}}\sigma_c\tau(v^{-k}) \\ &= \mathrm{ord}_{\mathfrak{R}}\tau(v^{-kc}) \\ &= kc. \end{aligned}$$

As c ranges over $(\mathbf{Z}/m\mathbf{Z})^*$ each conjugate of $\mathfrak{R}$ appears once. This finishes the proof.

1.2.3 Idempotents

Let G be a finite Abelian group and χ an element of the character group. The *orthogonal idempotent* is defined by

$$\varepsilon_\chi = \frac{1}{|\,G\,|}\sum_{\sigma\in G}\chi(\sigma)\sigma^{-1} \in \bar{\mathbf{Q}}[G].$$

For an irreducible $\mathbf{Z}_p$-representation Ξ, I will use the notation ε_Ξ to denote

$$\frac{1}{|\,G\,|}\sum_{\sigma\in G}\mathrm{Tr}\;\Xi(\sigma)\sigma^{-1} \in \mathbf{Z}_p[G].$$

We have the following properties (see [W]):

i). $\varepsilon_\chi^2 = \varepsilon_\chi$,

ii). $\varepsilon_\chi\varepsilon_\psi = 0$ if $\chi \neq \psi$,

iii). $\sum_{\chi\in\hat{G}}\varepsilon_\chi = 1$,

iv). $\sigma\varepsilon_\chi = \chi(\sigma)\varepsilon_\chi$.

Let M be a module over $\bar{\mathbf{Q}}[G]$, then we can decompose M as follows:

$$M = \oplus_\chi M_\chi, \text{ where } M_\chi = \varepsilon_\chi M.$$

Every M_χ is an eigenspace with the eigenvalue $\chi(\sigma)$. All the above works if $\bar{\mathbf{Q}}$ is replaced by any commutative ring which contains all the values of $\chi \in \hat{G}$ and in which $|\,G\,|$ is invertible.

1.3 Notations and definitions

From now on we use the following notation. Fix M a large power of an odd prime p and let $F = \mathbf{Q}(\zeta_d)$ with $p \mid d$ and $p \nmid \phi(d)$. Let S be the set of positive squarefree integers which are divisible only by primes l which split completely in F and in $\mathbf{Q}(\zeta_M)$.
For every $r \equiv 1 \bmod d$ write $G_r = \mathrm{Gal}(F(\zeta_r)/F)$. If $l \equiv 1 \bmod d$, l

prime and $l \nmid r$, then we identify G_l with $\mathrm{Gal}(F(\zeta_{rl})/F(\zeta_r))$. We write Fr_l for the Frobenius of l in G_r, the automorphism which sends each r-th root of unity to its l-th power.
Write $N_r = \sum_{\tau \in G_r} \tau$. Fix a generator σ_l of G_l and define

$$D_l = \sum_{i=1}^{l-2} i\sigma_l^i \in \mathbf{Z}[G_l].$$

Then

$$(\sigma_l - 1)D_l = (l-1) - N_l.$$

For $n \in S$ define

$$D_n = \prod_{l|n} D_l \in \mathbf{Z}[G_n].$$

Write $G = \mathrm{Gal}(F/\mathbf{Q})$. If $(n,d) = 1$ we can view G as a subgroup of $\mathrm{Gal}(F(\zeta_n)/\mathbf{Q})$ through the isomorphism

$$\mathrm{Gal}(F/\mathbf{Q}) \cong \mathrm{Gal}(F(\zeta_n)/\mathbf{Q}(\zeta_n)).$$

Let A denote the p-part of the ideal class group of F.

Definition 1.5 *For $n \in S, r \equiv 1$ mod dn is prime, and $\mathfrak{r}$ a prime of $F(\zeta_n)$ with $\mathfrak{r} \mid r$ the Gauss sum is defined by*

$$g(n, \mathfrak{r}, \zeta_r) = \sum_{a=1}^{r-1} \varepsilon_{n,\mathfrak{r}}(a)\zeta_r^a \in F(\zeta_{nr})^*,$$

where $\varepsilon_{n,\mathfrak{r}}$ is a character of $\mathbf{F}_r^*$ defined by

$$\varepsilon_{n,\mathfrak{r}} = \upsilon_{\mathfrak{r}}^{-(r-1)/dn}.$$

In other words

$$\varepsilon_{n,\mathfrak{r}} : (\mathbf{Z}/r\mathbf{Z})^* \to \mu_{dn}$$

is the character satisfying

$$\varepsilon_{n,\mathfrak{r}}(a) \equiv a^{-(r-1)/dn} \bmod \mathfrak{r}.$$

Let $O = \mathbf{Z}_p[\zeta_{\phi(d)}] \subseteq \mathbf{Q}_p(\zeta_{\phi(d)})$.
For a $\mathbf{Z}_p[G]$ module B define the action of G on the $O[G]$-module $O \otimes B$ by $\sigma(o \otimes b) = o \otimes \sigma(b)$. Unless specified otherwise $\otimes$ is taken over $\mathbf{Z}_p$.

Let Ξ be an irreducible $\mathbf{Z}_p$ representation of G. If we regard Ξ as an O representation, we may write $\Xi = \sum \rho_i$, where ρ_i is a linear odd character of G for all i.
Using the isomorphism

$$G \cong \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{Q}(\zeta_{d/p})/\mathbf{Q}),$$

we can write $\rho_i = \omega^j \times \psi$, where ψ is a linear character of $\mathbf{Q}(\zeta_{d/p})$.

Lemma 1.2 *It is possible to choose a c_1 such that $\rho_i(\sigma_c) - c_1 \in O^*$ as long as $\rho_i \neq \omega \times 1$.*

Remark 1.1 If $\rho_i = \omega \times \psi$ we have to fix a different automorphism.

Proof. First assume that $j \not\equiv 1 \bmod p-1$ then proceed as in [G]. Note that $c_1 \equiv c \bmod d$. Using the Chinese Remainder Theorem, we choose a $c \in \mathbf{Z}$, such that $c \equiv a \bmod p$, with a a primitive root of $(\mathbf{Z}/p\mathbf{Z})^*$ and $c \equiv 1 \bmod \frac{d}{p}$. This gives us

$$\begin{aligned} \omega^j(\sigma_c)\psi(\sigma_c) - c_1 &= \omega^j(c) \times \psi(c) - c_1 \\ &= \omega^j(a) \times \psi(1) - c_1 \\ &\equiv a^j - a \bmod p. \end{aligned}$$

If $j \equiv 1 \bmod p-1$ then we choose the automorphism σ_b which leaves $\mathbf{Q}(\zeta_p)$ fixed and $\psi(b) \neq 1$. In this way we get

$$\omega(\sigma_b)\psi(\sigma_b) - b_1 \equiv \psi(b) - 1 \bmod p.$$

From now on assume that $\rho_i \neq \omega \times 1$.

Fix a $\sigma_c \in G$ where σ_c, $(c,d) = 1$, denotes the element of G which maps ζ_d to ζ_d^c and choose $\forall\, n \in S$ a c_n such that

i). $\zeta^{\sigma_c} = \zeta^{c_n}\ \forall\ \zeta \in \mu_{Mdn}$,

ii). $\rho_i(\sigma_c) - c_1 \in O^*$.

Definition 1.6 *For $n \in S$ write $\tau_a \in Gal(F(\zeta_n)/\mathbf{Q})$ for the automorphism which sends each $\zeta \in F(\zeta_n)$ to ζ^a. Define the* Stickelberger element *by*

$$s(n) = \sum_{a=1,(a,dn)=1}^{dn} a\tau_a^{-1} \in \mathbf{Z}[Gal(F(\zeta_n)/\mathbf{Q})],$$

and define

$$\theta(n) = \frac{1}{dn}(\sigma_c - c_n)s(n),$$

$$\theta(n,\Xi) = \varepsilon_\Xi\theta(n).$$

We have $\theta(n) \in \mathbf{Z}[\mathrm{Gal}(F(\zeta_n)/\mathbf{Q})]$ (see [W]), since

$$\begin{aligned} &\sum_{a=1,(a,dn)=1}^{dn} [\tfrac{a}{dn}]\sigma_c\tau_a^{-1} - \sum_{a=1,(a,dn)=1}^{dn} c_n[\tfrac{a}{dn}]\tau_a^{-1} \\ = &\sum_{a=1,(a,dn)=1}^{dn} ([\tfrac{ac_n}{dn}] - [\tfrac{a}{dn}]c_n)\tau_a^{-1}, \end{aligned}$$

so $\theta(n,\Xi) \in \mathbf{Z}_p[\mathrm{Gal}(F(\zeta_n)/\mathbf{Q})]_\Xi$.

Definition 1.7 *Let $n \in S$, $\mathfrak{r}$ a prime of $F(\zeta_n)$, with $\mathfrak{r} \mid r \equiv 1$ mod dn. Then*

$$\alpha(n,\mathfrak{r}) = g(n,\mathfrak{r},\zeta_r)^{\sigma_c - c_n}.$$

Remark 1.2 This definition depends on the choice of σ_c.

For a $\sigma = \sigma_a \in G_r$ we have

$$g(n,\mathfrak{r},\zeta_r)^\sigma = g(n,\mathfrak{r},\zeta_r^\sigma) = \varepsilon_{n,\mathfrak{r}}(\sigma)^{-1}g(n,\mathfrak{r},\zeta_r),$$

where $\varepsilon_{n,\mathfrak{r}}(\sigma)$ should be interpreted as $\varepsilon_{n,\mathfrak{r}}(a)$.

This gives

$$\alpha(n,\mathfrak{r})^{\sigma} = (\varepsilon_{n,\mathfrak{r}}(\sigma)^{-1})^{\sigma_c - c_n}\alpha(n,\mathfrak{r}).$$

Since $\sigma_c - c_n$ annihilates μ_{dn}, it follows that $\alpha(n,\mathfrak{r}) \in F(\zeta_n)^*$. This also shows that the definition of $\alpha(n,\mathfrak{r})$ is independent of the choice of ζ_r.

In the next section we will see that these elements form an Euler system. Furthermore we construct from $\alpha(n,\mathfrak{r})$ elements $\kappa(n,\rho)$ which give principal ideals in F which can be viewed as a relation in the ideal class group of F. These relations will be used to bound the size of the ideal class group.

1.4 Constructing principal ideals and relations

The next proposition makes clear why the Gauss sums form an Euler system and gives the ideal factorization of $\alpha(n,\mathfrak{r})$.

Proposition 1.1 *Let $n \in S$, $\mathfrak{r}$ a prime of $F(\zeta_n)$, $\mathfrak{r} \mid r \equiv 1$ mod dn.*

i). If l is a prime dividing n , then

$$\alpha(n,\mathfrak{r})^{N_l} = \alpha(n/l, N_l\mathfrak{r})^{1-Fr(l)^{-1}}\beta^M$$

for some $\beta \in F(\zeta_{n/l})^*$,

ii). $(\alpha(n,\mathfrak{r})) = \theta(n)\mathfrak{r}$.

Proof. We have by definition

$$\alpha(n,\mathfrak{r})^{N_l} = \prod_{\sigma\in G_l}(\sum_{a=1}^{r-1}\varepsilon_{n,\mathfrak{r}}^{\sigma}(a)\zeta_r^a)^{\sigma_c - c_n}.$$

Using $\varepsilon_{n,\mathfrak{r}}^{l} = \varepsilon_{\frac{n}{l},N_l\mathfrak{r}}$ gives

i). $\varepsilon_{n,\mathfrak{r}}^{\sigma-1}$ is a character of order l since $(\varepsilon_{n,\mathfrak{r}}^{l})^{\sigma-1} = (\varepsilon_{\frac{n}{l},N_l\mathfrak{r}})^{\sigma-1} = 1$,

ii). $\varepsilon_{n,\mathfrak{r}} = (\varepsilon_{\frac{n}{l},N_l\mathfrak{r}})^{Fr(l)^{-1}}$.

Thus we can write

$$\prod_{\sigma\in G_l}(\sum_{a=1}^{r-1}\varepsilon_{n,\tau}^{\sigma}(a)\zeta_r^a)=g(\frac{n}{l},N_l\tau,\zeta_r^l)^{-Fr(l)^{-1}}\prod_{\psi:G_r\to\mu_l}(\sum_{a=1}^{r-1}\psi\varepsilon_{n,\tau}(a)\zeta_r^a).$$

Now we use the Davenport-Hasse distribution relation (see preliminaries):

$$\prod_{\psi^l=1}\tau(\psi\chi)=-\tau(\chi^l)\chi(l^{-l})\prod_{\psi^l=1}\tau(\psi).$$

This gives

$$\prod_{\psi:G_r\to\mu_l}(\sum_{a=1}^{r-1}\psi\varepsilon_{n,\tau}(a)\zeta_r^a)=g(\frac{n}{l},N_l\tau,\zeta_r)\varepsilon_{n,\tau}(l^{-l})r^{(l-1)/2}.$$

Here we used $\varepsilon_{n,\tau}^l=\varepsilon_{\frac{n}{l},N_l\tau}$ and $\tau(\psi)\tau(\bar{\psi})=\psi(-1)r$.
Putting everything together we obtain

$$\alpha(n,\tau)^{N_l}=(g(\frac{n}{l},N_l\tau,\zeta_r)^{1-Fr(l)^{-1}}\varepsilon_{n,\tau}(l)^{1-l}r^{(l-1)/2})^{\sigma_c-c_n}.$$

Since $n\in S$ it follows that $M\mid(l-1)/2$ and
$(g(\frac{n}{l},N_l\tau,\zeta_r)^{1-Fr(l)^{-1}})^{c_n-c_{n/l}}\in F(\zeta_{n/l})^M$ since $Mn/l\mid(c_n-c_{n/l})$.

For (ii) use the ideal factorization (see lemma 1.1)

$$(g(n,\tau,\zeta_r)^{\sigma_c-c_n})=\mathfrak{r}^{\frac{1}{dn}(\sigma_c-c_n)s(n)}.$$

Until now we were dealing with elements in an extension field of F. The following lemma demonstrates how to obtain elements in F.

Lemma 1.3 *Let Ξ be an irreducible $\mathbf{Z}_p$ representation of $Gal(F/\mathbf{Q})$ such that the character afforded by Ξ is not equal to $\omega\times 1$ and let F'/F be Abelian over $\mathbf{Q}$. Then we have an isomorphism*

$$(F^*/(F^*)^M)_\Xi\cong((F'^*/(F'^*)^M)^{Gal(F'/F)})_\Xi.$$

Proof. For $\Xi \neq \omega \times 1$ we have an exact sequence

$$0 \to (F^*)_\Xi \to (F^*)_\Xi \to (F^*/F^{*M})_\Xi \to 0.$$

For $G = \mathrm{Gal}(F'/F)$ we also have the exact sequence

$$0 \to (F'^*)_\Xi^G \to (F'^*)_\Xi^G \to (F'^*/F'^{*M})_\Xi^G \to H^1(F'/F, F'^*)_\Xi.$$

This gives us using Hilbert 90 and $(F'^*)_\Xi^G = (F^*)_\Xi$

$$(F^*/F^{*M})_\Xi \cong (F'^*/F'^{*M})_\Xi^G.$$

From now on assume that the character afforded by Ξ is not equal to $\omega \times 1$

Lemma 1.4 *If $n \in S$ and $\mathfrak{r}$ a prime of $F(\zeta_n)$, $\mathfrak{r} \mid r \equiv 1 \bmod dn$. Then*

i). $\alpha(n,\mathfrak{r})^{D_n} \in [F(\zeta_n)^*/(F(\zeta_n)^*)^M]^{G_n}$,

ii). $D_n\theta(n) \in \mathbf{Z}/M\mathbf{Z}[Gal(F(\zeta_n)/\mathbf{Q})]^{G_n}$.

For a proof see Rubin ([Ru2]).
Note that since r splits completely we have

$$(\oplus_{\mathfrak{r}|r}\mathbf{Z}/M\mathbf{Z}\ \mathfrak{r})^{G_n} = \mathbf{Z}/M\mathbf{Z}[\mathrm{Gal}(F(\zeta_n)/\mathbf{Q})]^{G_n}.$$

Definition 1.8 *Take $F' = F(\zeta_n)$, and let $n \in S$, $\mathfrak{r}$ be a prime of $F(\zeta_n)$, ρ be a prime of F with $\mathfrak{r} \mid \rho \mid r \equiv 1 \bmod dn$.*
Then $\kappa(n,\rho) \in (F^*/(F^*)^M)_\Xi$ is defined as the image of $\varepsilon_\Xi \alpha(n,\mathfrak{r})^{D_n}$ under the above isomorphism.

This image depends on ρ, and not on $\mathfrak{r}$.

We have

$$(\oplus_{\sigma \in \mathrm{Gal}(F(\zeta_n)/\mathbf{Q})}\mathbf{Z}/M\mathbf{Z}\ \mathfrak{r}^\sigma)^{G_n} = (\oplus_{\tau \in \mathrm{Gal}(F/\mathbf{Q})}\mathbf{Z}/M\mathbf{Z}\ \rho^\tau)^{N_n}$$

equivalently

$$\mathbf{Z}/M\mathbf{Z}[\mathrm{Gal}(F(\zeta_n)/\mathbf{Q})]^{G_n} = N_n\mathbf{Z}/M\mathbf{Z}[\mathrm{Gal}(F/\mathbf{Q})].$$

This leads to the following definition.

Definition 1.9 *Define* $\delta(n) \in \mathbf{Z}/M\mathbf{Z}[Gal(F/\mathbf{Q})]_\Xi$ *such that*

$$D_n\theta(n,\Xi) = \delta(n)N_n.$$

Define $d(n)$ *to be the largest divisor of* M *which divides* $\delta(n)$.

These $d(n)$'s provide us, for suitable n, with annihilators of ideal classes of the Ξ components of the ideal class group as will appear at the end of this chapter.
First we have to take a closer look at the ideal factorization of $\kappa(n,\rho)$. The following notation is used. Write I for the group of fractional ideals of F, so $I = \oplus_l I_l = \oplus_l \oplus_{\lambda|l} \mathbf{Z}\lambda$. Let (y) denote the principal ideal and let $[y]$ respectively $[y]_l$ be the projection in I/MI respectively I_l/MI_l.

Proposition 1.2 $\forall\ n \in S$ *and primes* ρ *of* F *with* $\rho \mid r \equiv 1 \bmod dn$, *there is a unique* $\kappa(n,\rho) \in (F^*/(F^*)^M)_\Xi$ *such that*

i). $\kappa(n,\rho) \equiv \alpha(n,\mathfrak{r})^{\varepsilon_\Xi D_n} \bmod (F(\zeta_n)^*)^M$ *for every* $\mathfrak{r}$ *of* $F(\zeta_n)$ *above* ρ,

ii). $[\kappa(n,\rho)] = \delta(n)\rho + \sum_{l|n}[\kappa(n,\rho)]_l$ *in* I/MI.

Proof. All primes not dividing n are unramified in $F(\zeta_n)/F$ and $(\alpha(n,\mathfrak{r})) = \theta(n)\mathfrak{r}$. So if $l \nmid nr$ then $[\kappa(n,\rho)]_l = 0$.

Definition 1.10 *Let* g_l *be a primitive root of* $(\mathbf{Z}/l\mathbf{Z})^*$ *corresponding to the chosen generator* σ_l *of* G_l. *For* K *a number field, let* λ *be a prime of* K *of degree 1 lying above* l. *Define*

$$\nu_\lambda : \{y \in F^* : ord_\lambda(y) = 0\} \to \mathbf{Z}/(l-1)\mathbf{Z}$$

by $g_l^{\nu_\lambda(u)} \equiv u \bmod \lambda$.

If $l \in S$ and λ a prime of F above l, extend this map to

$$\phi_\lambda : \{y \in F^*/(F^*)^M : [y]_l = 0\} \to \mathbf{Z}/M\mathbf{Z}[G]$$

by

$$\phi_\lambda(y) \equiv \sum_{\sigma \in G} \nu_{\lambda^\sigma}(\bar{y})\sigma \bmod M,$$

where $\bar{y}$ is a lift of y to F^* which is prime to l.

Theorem 1.1 *Let $n \in S$ and let ρ, ρ' be primes of F lying above distinct primes $r \equiv r' \equiv 1 \bmod nd^2M$. Let $A(n)$ be the p-part of the ideal class group of $F(\zeta_n)$, and suppose that there are primes $\mathfrak{r}, \mathfrak{r}'$ of $F(\zeta_n)$, above ρ, ρ' whose projections into $A(n)_\Xi$ are the same. Then*

$$\phi_\rho(\kappa(n, \rho')) \equiv \delta(nr) \bmod \delta(n)\mathbf{Z}/M\mathbf{Z}[G]_\Xi.$$

The results needed for proving this theorem are stated below. The proofs are similar as in Rubin, only prop. 1.4 (prop. 2.8 [Ru2]) needs an addition. Prop. 1.3 (prop. 2.7 [Ru2]) shall be explained, since this is the key result for the proof of this theorem.

Lemma 1.5 *Suppose $m \in \mathbf{Z}$ and $r \in S$ is prime, $r \equiv 1 \bmod 2m$. Write $t = (r-1)/m$. Then for every a, $1 \le a \le m-1$, such that $(a, m) = 1$, we have*

$$\sum_{b=1, b \equiv a \bmod m, r \nmid b}^{mr} b\nu_r(b) \equiv x + m\nu_r(-1/(at)!) \bmod t/2.$$

Definition 1.11 *For $n \in \mathbf{Z}, r \equiv 1 \bmod mnd$, r prime, define elements of $\mathbf{Z}/M\mathbf{Z}[Gal(F(\zeta_n)/\mathbf{Q})]$ by*

$$s'(n, r) \equiv \sum_{a \in \mathbf{Z}, (a, dn)=1}^{dn} \nu_r(-1/(at)!)\tau_a^{-1} (\bmod M),$$

$$\theta'(n, r, \Xi) = \varepsilon_\Xi(c_n - \sigma_c)s'(n, r),$$

where $t = (r-1)/dn$.

We have the following relation:

Lemma 1.6 *If $n \in S$ and $r \equiv 1 \bmod nd^2M$, then*

$$D_r\theta(nr,\Xi) = \theta'(n,r,\Xi)N_r \text{ in } \mathbf{Z}/M\mathbf{Z}[Gal(F(\zeta_{nr})/\mathbf{Q})].$$

Remark 1.3 If we take $n = 1$ and q a prime congruent to 1 mod d^2M. Then

$$D_q\theta(q,\Xi) = \theta'(1,q,\Xi)N_q.$$

Recall $\delta(q)N_q = D_q\theta(q,\Xi)$. So we can compute $\delta(q)$ since $\delta(q) = \theta'(1,q,\Xi)$.

We will see later that a Ξ component of the ideal class group is cyclic (as $\mathbf{Z}_p[G]_\Xi$ module) if and only if there exists a prime $q \in S$ such that $d(q) = 1$.

The next proposition gives the connection between the ideal factorization and the residue classes modulo the next higher power of each prime divisor of Gauss sums.

Proposition 1.3 *Suppose $n \in S$ and ρ a prime of F such that $\rho \mid r \equiv 1 \bmod nd^2M$. Then there is a $\pi \in F^*$ such that $[\pi]_r = \rho$, $[\kappa(n,\rho)/\pi^{\delta(n)}]_r = 0$, and*

$$\phi_\rho(\kappa(n,\rho)/\pi^{\delta(n)}) = \delta(nr).$$

Proof. Fix a primitive r-th root of unity ζ_r, and a prime $\mathfrak{r}$ in $F(\zeta_n)$ above ρ. Write $\mathfrak{R}$ for the prime of $F(\zeta_{nr})$ above $\mathfrak{r}$. Use the Chinese Remainder Theorem to fix an element Π of $(F(\zeta_{nr}))^*$, integral at all primes above r, such that

$$\Pi \equiv \zeta_r - 1 \bmod \mathfrak{R}^2 \text{ and } \Pi \equiv 1 \bmod \mathfrak{R}^\tau$$

for all $\tau \neq 1$ in $\mathrm{Gal}(F(\zeta_n)/\mathbf{Q})$.

Let $\tau = \tau_a \in \mathrm{Gal}(F(\zeta_n)/\mathbf{Q})$ act on μ_{dn} by $\zeta \to \zeta^a$ and suppose $t = \frac{r-1}{dn}$, then (see lemma 1.1)

$$\mathrm{ord}_{\mathfrak{R}^{\tau-1}}(g(n,\mathfrak{r},\zeta_r)) = \mathrm{ord}_{\mathfrak{R}}(g(n,\mathfrak{r},\zeta_r))^{\tau} = at.$$

From $\Pi \equiv \zeta_r - 1 \bmod \mathfrak{R}^2$ follows $\mathrm{ord}_{\mathfrak{R}}(\Pi) = 1$, since $F(\zeta_{nr})/F(\zeta_r)$ is unramified at r. Equivalently, $\mathrm{ord}_{\mathfrak{R}^{\tau-1}}(\Pi^{\tau^{-1}}) = 1$.

This gives us

$$(g(n,\mathfrak{r},\zeta_r))/(\Pi^{\tau^{-1}})^{at} \equiv \frac{-1}{(at)!} \bmod \mathfrak{R}^{\tau^{-1}}.$$

Since $\Pi^{\tau_b^{-1}} \equiv 1 \bmod \mathfrak{R}^{\tau_a^{-1}}$ for all $a \neq b$, we also have

$$(g(n,\mathfrak{r},\zeta_r))/(\Pi^{\tau^{-1}})^{at} \equiv (g(n,\mathfrak{r},\zeta_r))/(\Pi^{s(n)t}).$$

Define a Galois-equivariant map

$$\psi : \{y \in (F(\zeta_{nr}))^* : y \text{ is prime to } r \to \mathbf{Z}/M\mathbf{Z}[\mathrm{Gal}(F(\zeta_n)/\mathbf{Q})]\}$$

by

$$\psi(y) \equiv \sum_{\tau \in \mathrm{Gal}(F(\zeta_n)/\mathbf{Q})} \nu_{\mathfrak{R}^{\tau}}(y)\tau \bmod M.$$

By the definition of $s'(n,r)$:

$$\psi((g(n,\mathfrak{r},\zeta_r))/(\Pi^{s(n)t})) = s'(n,r).$$

Apply $\varepsilon_{\Xi}(\sigma_c - c_n)N_r$ to both sides and use lemma 1.6, then

$$\begin{aligned} \varepsilon_{\Xi}\psi(\alpha(n,\mathfrak{r})/\Pi^{(r-1)\theta(n)})N_r &= \theta'(n,r,\Xi)N_r \\ &= D_r\theta(nr,\Xi). \end{aligned}$$

We have for $y \in F^*$ prime to r, $\psi(y) = \phi_\rho(y)N_n$, because $\nu_{\mathfrak{r}^\sigma}(y) = \nu_{\mathfrak{r}}(y)$ for all $\sigma \in F(\zeta_n)/F$. If we apply D_n to both sides we get

$$\psi(\kappa(n,\rho)/\Pi_0^{\delta(n)N_n}) = \delta(nr)N_n.$$

Π_0 is defined as follows: From $\mathrm{ord}_{\mathfrak{R}}(\Pi) = 1$ follows $\mathrm{ord}_{\mathfrak{r}}(\Pi^{r-1}) = 1$. Choose $\Pi_0 \in F(\zeta_n)^*$ such that $\mathrm{ord}_{\mathfrak{r}}(\Pi_0) = 1$ and $\mathrm{ord}_{\mathfrak{r}^{\tau'}}(\Pi_0) = 0$ for $\tau' \in \mathrm{Gal}(F(\zeta_n)/F), \tau' \neq 1$. Then $\mathrm{ord}_{\rho}(\Pi_0^{N_n}) = 1$ and $\mathrm{ord}_{\rho^{\sigma}}(\Pi_0^{N_n}) = 0$ for $\sigma \in \mathrm{Gal}(F/\mathbf{Q}), \sigma \neq 1$. Define $\pi = \Pi_0^{N_n}$, then

$$\phi_{\rho}(\kappa(n,\rho)/\pi^{\delta(n)}) = \delta(nr).$$

This finishes the proof.

Proposition 1.4 *Suppose $n \in S$ and ρ, ρ' are primes of F lying above distinct rational primes $r \equiv r' \equiv 1 \bmod nd^2M$. Let $A(n)$ be the p-part of the ideal class group of $F(\zeta_n)$ and suppose that there are primes $\mathfrak{r}, \mathfrak{r}'$ above ρ, ρ', whose projections into $A(n)_{\Xi}$ are the same. Then*

$$\kappa(n,\rho')/\kappa(n,\rho) \in (F^*)^{\delta(n)}(F^*)^M/(F^*)^M.$$

Proof. The proof is similar as in Rubin ([Ru2]) with the addition that $(E/E^M)_{\Xi}$ is trivial if the character afforded by Ξ is not equal to $\omega \times 1$, where E denotes the group of units in $F(\zeta_n)$ (See [G]).

Let $A(n)$ be the p-part of the ideal class group of $F(\zeta_n)$ and Ξ an irreducible $\mathbf{Z}_p$ representation of G. Recall that the character afforded by Ξ is not equal to $\omega \times 1$. We have the following application of Chebotarev which gives us the final ingredient to construct all the relations we need in the ideal class group.

Theorem 1.2 *Suppose k and n are positive integers, $c \in A(n)_{\Xi}$, $\beta \in (F^*/(F^*)^M)_{\Xi}$, t the largest divisor of M such that $\beta \in (F^*)^t/(F^*)^M$. Then there are infinitely many primes λ of F, with $\lambda \mid l$ such that:*

i). There is a prime of $F(\zeta_n)$ above λ whose projection into $A(n)_{\Xi}$ is c,

ii). $l \equiv 1 \bmod Mkn$,

iii). $[\beta]_l = 0$ and there is a $u \in (\mathbf{Z}/M\mathbf{Z})^*$ such that $\phi_{\lambda}(\beta) = ut\varepsilon_{\Xi}$.

Proof. The proof is similar to Rubin ([Ru2]) with the addition that $\Xi \neq \hat{\Xi} \otimes \omega$ where $\hat{\Xi}$ denotes the contragredient (see property ix of the group representations), since G does not have a character ξ with $\xi^2 = \omega$. See also [Ru 4].

1.5 The minus class group

1.5.1 Bernoulli numbers

Definition 1.12 *The ordinary* Bernoulli numbers *are defined by*

$$\sum_{n=0}^{\infty} B_n \frac{t^n}{n!} = \frac{t}{e^t - 1}.$$

The generalized Bernoulli numbers *are defined by*

$$\sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!} = \sum_{a=1}^{f_\chi} \frac{\chi(a) t e^{at}}{e^{f_\chi t} - 1}.$$

We have the following properties:

i). For $\chi = 1$ and $n \neq 1$ we obtain the ordinary Bernoulli numbers,

ii). If $n = 1$ we have $B_{1,1} = \frac{1}{2}$ and $B_1 = -\frac{1}{2}$,

iii). If χ is not trivial with conductor f then $B_{1,\chi} = \frac{1}{f} \sum_{a=1}^{f} \chi(a) a$, if $f \mid n$ then $\frac{1}{n} \sum_{a=1}^{n} \chi(a) a = \frac{1}{f} \sum_{a=1}^{f} \chi(a) a$,

iv). The defining relation for the $B_{n,\chi}$ is an even function of t when χ is even, and odd when χ is odd. Therefore $B_{n,\chi} = 0$ if $n \not\equiv \delta_\chi \bmod 2$ with the exception of $n = 1$,

v). Let X be a group of Dirichlet characters and K the associated field. Assume K is totally complex, then we have the class number formula (see [W])

$$h^-(K) = Qw \prod_{\chi \in X, \chi \text{ odd}} (-\frac{1}{2} B_{1,\chi}),$$

where w denotes the number of roots of unity in K and $Q = 1$ or 2.

1.5.2 Orders of Ξ components

Lemma 1.7 *If Ξ is an irreducible $\mathbf{Z}_p$ representation of G and $\Xi = \sum_i \rho_i$, then*

$$\varepsilon_\Xi = \sum_i \varepsilon_{\rho_i}.$$

Proof.

$$\begin{aligned}\varepsilon_\Xi &= \frac{1}{|G|}\sum_\tau Tr(\Xi(\tau))\tau^{-1} \\ &= \frac{1}{|G|}\sum_\tau \sum_i Tr(\rho_i(\tau))\tau^{-1} \\ &= \sum \varepsilon_{\rho_i}.\end{aligned}$$

As before we assume that the character afforded by Ξ is not equal to $\omega \times 1$. Recall

$$\delta(n) \in \mathbf{Z}/M\mathbf{Z}[G]_\Xi \subseteq O/MO[G]_\Xi.$$

If we decompose $O/MO[G]_\Xi$ in linear components we see that $d(n) = d_i(n)$ for all i, where $d_i(n)$ is the largest divisor of M which divides $\delta_i(n) \in O/MO[G]_{\rho_i} \cong O/MO\varepsilon_{\rho_i}$. In fact the ρ_i components of an $(O[G])_\Xi$ module are isomorphic (see chapter 2). By definition

$$\delta(1) = \varepsilon_\Xi(\sigma_c - c_1)s(1).$$

This gives us

$$\begin{aligned}\delta_i(1) &= \varepsilon_{\rho_i}(\sigma_c - c_1)\sum_{(a,d)=1}\frac{a}{d}\tau_a^{-1} \\ &= (\rho_i(\sigma_c) - c_1)B_{1,\rho^{-1}}\varepsilon_{\rho_i}.\end{aligned}$$

If the conductor of ρ_i is less than d, use property (iii) of the Bernoulli numbers.
Since $\rho_i \neq \omega \times 1$ we have $\rho_i(\sigma_c) - c_1 \in O^*$. This implies

$$\delta_i(1)O/MO = B_{1,\rho^{-1}}O/MO,$$

since $B_{1,\psi} \in O$ if $\psi \neq (\omega \times 1)^{-1}$. Now we can proceed as in Rubin ([Ru2]) which gives us the following theorem.

Theorem 1.3 *Suppose* $d(1)\#(A_\Xi)p \mid M$, $n \in S$, *and* $c \in A_\Xi$. *Let* B *denote the subgroup of* A *generated by the classes of primes of* F *dividing* n. *If* $d(n) \mid d(1)$ *and* $c \notin B_\Xi$, *then there is a prime* λ *of* F *lying above* $l \in S$ *such that*

i). The projection of the class of λ *into* A_Ξ *is* c,

ii). $d(nl) \mid d(n)$ *and* $d(n)/d(nl)$ *annihilates* c *in* A_Ξ/B_Ξ.

Proof. See [Ru2]

Corollary 1.1 *Suppose* $d(1)\#(A_\Xi)p \mid M$ *and* $n \in S$. *Let* B *denote the subgroup of* A *generated by the classes of primes of* F *dividing* n. *Then*

$$\#(A_\Xi/B_\Xi) \mid d(n)^{\dim \Xi}.$$

For a proof see Rubin ([Ru2]). Note that if $\mathfrak{c}_1, \ldots, \mathfrak{c}_k \in A_\Xi$ generate A_Ξ/B_Ξ and c_i is the order of $\mathfrak{c}_i$ in $A_\Xi/(B_\Xi, \mathfrak{c}_1, \ldots, \mathfrak{c}_{i-1})$ then

$$\#(A_\Xi/B_\Xi) = \prod_i c_i^{\dim \Xi},$$

since $\mathbf{Z}_p[G]_\Xi$ is a free $\mathbf{Z}_p$ module of rank $\dim \Xi$.

If we take $n = 1$ we get

$$\#A_\Xi \mid d(1)^{\dim \Xi},$$

implying

$$\#(O \otimes A)_{\rho_i} \mid d_i(1)^{\mathbf{Z}_p \mathrm{rk} O} = (p^{ord_p B_{1,\rho_i^{-1}}})^{\mathbf{Z}_p \mathrm{rk} O}.$$

Lemma 1.8 *If the character afforded by the irreducible* $\mathbf{Z}_p$ *representation* Ξ *of* G *is equal to* $\omega \times 1$, *then* $\#A_\Xi = 1$.

Proof. Let $K = \mathbf{Q}(\zeta_p)$ and $N = \mathrm{Gal}(F/K)$ then,

$$\begin{aligned}
\varepsilon_{\omega\times 1} &= \frac{1}{G}\sum_{\sigma\in \mathrm{Gal}(F/\mathbf{Q})} \omega\times 1(\sigma^{-1})\sigma \\
&= \frac{|N|}{|G|}\Big(\sum_{\tau\in \mathrm{Gal}(K/\mathbf{Q})} \omega(\tau^{-1})\tau\Big) N_{F/K} \\
&= \frac{|N|}{|G|}\varepsilon_\omega N_{F/K}.
\end{aligned}$$

By composing $A_K \to A \to A_K$ we have an isomorphism which sends $[a]$ to $[a]^{\phi(d/p)}$, so $N_{F/K}A = A_K$.
Now use the well-known fact (see [W]) that $(A_K)_\omega$ is annihilated by $pB_{1,\omega^{-1}} \equiv p-1 \bmod p$.

For $a, b \in \mathbf{Z}_p$ write $a \sim b$ for $a/b \in \mathbf{Z}_p^*$.
Put everything together and use the class number formula to obtain:

Theorem 1.4 *For every odd character $\chi \neq \omega\times 1$ of G,*

$$\#(O\otimes A)_\chi = (p^{ord_p B_{1,\chi^{-1}}})^{\mathbf{Z}_p \mathrm{rk} O}.$$

Proof.

$$\begin{aligned}
\prod_{\chi odd, \chi\neq\omega\times 1} \#(O\otimes A)_\chi &= \prod_{\chi odd} \#(O\otimes A)_\chi \\
&= \#(O\otimes A^-) \\
&\sim (p\prod_{\chi \text{ odd}} B_{1,\chi})^{\mathbf{Z}_p \mathrm{rk} O} \\
&\sim (\prod_{\chi \text{ odd}, \chi\neq\omega\times 1} B_{1,\chi^{-1}})^{\mathbf{Z}_p \mathrm{rk} O}.
\end{aligned}$$

So for all χ odd with $\chi \neq \omega\times 1$ we have

$$\#(O\otimes A)_\chi = (p^{\mathrm{ord}_p B_{1,\chi^{-1}}})^{\mathbf{Z}_p \mathrm{rk} O}.$$

From this theorem and the proof of the corollary it follows that

$$\#A_\Xi = d(1)^{\dim \Xi},$$

and using the same notation as in [Ru2], $c_i = (d(n_{i-1})/d(n_i))$ for every i, and $d(n_k) = 1$ (see the remark made after th. 4.3 [Ru2]). This gives us a criterion to determine whether a χ component of the ideal class group is cyclic with χ linear.

Lemma 1.9 *Let Ξ be an irreducible $\mathbf{Z}_p$ representation, with $\Xi = \sum \rho_i$. Take $M = pd(1)^{(dim\ \Xi)+1}$ or larger. Then*

$$(O \otimes A)_{\rho_i} \text{ is cyclic } \Leftrightarrow \text{ there is a prime } q \in S \text{ with } d_i(q) = 1.$$

Proof. If A_Ξ is generated by one prime, then there is a prime $q \in S$ such that $d(q) = d(n_1) = 1$ (take $n = 1$ in the proof of corollary 4.2 of [Ru2]). Suppose B is the subgroup of A generated by the classes of primes of F above q, where q is a prime such that $q \in S$ and $d(q) = 1$. Then

$$\#(A_\Xi/B_\Xi) \mid d(q)^{\dim \Xi} = 1,$$

which means that A_Ξ is generated by primes above q, so every linear component is cyclic.

If we take a prime q congruent to 1 mod d^2M, we have $\delta(q) = \theta'(1, q, \Xi)$ (see remark 1.3). This gives us using $\rho_i(\sigma_c) - c_1 \in O^*$,

$$d_i(q)O/MO = (\sum_{a \in \mathbf{Z}, (a,d)=1}^{d} \nu_q(-1/(at)!)\rho_i^{-1}(a))O/MO.$$

Unfortunately the prime q is very large.

Note that in the same way the p-rank of A_Ξ can be computed.
If $n = lr$, $d(n) = 1$ and $d(l) \neq 1 \neq d(r)$, then A_Ξ is generated by primes above l and r so the p-rank equals 2 etc.

So far this chapter has been dealing with the ideal class group of $F = \mathbf{Q}(\zeta_d)$, where we assumed that p is a divisor of d. The next section will show that from this case we can deduce all other cases.

1.5.3 The general case

Lemma 1.10 *If $F = \mathbf{Q}(\zeta_d)$, $p \nmid d$ and ψ is an odd character of $\widehat{Gal(F/\mathbf{Q})}$, then*

$$\#(O \otimes A_F)_\psi = (p^{\mathrm{ord}_p B_{1,\psi^{-1}}})^{\mathbf{Z}_p \mathrm{rk} O}.$$

Proof. We simply adjoin ζ_p to F which gives us for $F' = \mathbf{Q}(\zeta_{pd})$ and for all χ odd with $\chi \neq \omega \times 1$

$$\#(O \otimes A_{F'})_\chi = (p^{\mathrm{ord}_p B_{1,\chi^{-1}}})^{\mathbf{Z}_p \mathrm{rk} O}.$$

Take $\chi = \psi \times 1$ with $\psi \in \widehat{\mathrm{Gal}(F/\mathbf{Q})}$, ψ odd. Then similarly as in the proof of lemma 1.8 the Norm is surjective so

$$\#(O \otimes A_{F'})_{\psi \times 1} = \#(O \otimes NA_{F'})_\psi = \#(O \otimes A_F)_\psi.$$

Also

$$\#(O \otimes A_{F'})_{\psi \times 1} = (p^{\mathrm{ord}_p B_{1,\psi^{-1} \times 1}})^{\mathbf{Z}_p \mathrm{rk} O} = (p^{\mathrm{ord}_p B_{1,\psi^{-1}}})^{\mathbf{Z}_p \mathrm{rk} O}.$$

Let $\mathrm{cond}(K)$ denote the minimal n such that $K \subseteq \mathbf{Q}(\zeta_n)$. This is possible since K is Abelian.

Proposition 1.5 *Let K be an arbitrary Abelian extension of $\mathbf{Q}$ with $p \nmid \phi(condK)$ and let ψ be an odd character of $\widehat{Gal(K/\mathbf{Q})}$. Then*

$$\#(O \otimes A_K)_\psi = (p^{\mathrm{ord}_p B_{1,\psi^{-1}}})^{\mathbf{Z}_p \mathrm{rk} O}.$$

Proof. Write $F = \mathbf{Q}(\zeta_{\mathrm{cond}(K)})$. Take a character ψ of $\hat{G} = \widehat{\mathrm{Gal}(F/\mathbf{Q})}$ with $\mathrm{Gal}(F/K) \subseteq \ker \psi$. Note that these characters form the character group of $\mathrm{Gal}(K/\mathbf{Q})$.
Write $G = \oplus_i \sigma_i N$, with $\sigma_i \in G/N$ then

$$\begin{aligned} \varepsilon_\psi &= \frac{1}{G} N_{F/K} \Big(\sum_{\sigma_i \in G/N} \psi(\sigma_i N) \sigma_i^{-1} \Big) \\ &= \frac{|N|}{|G|} N_{F/K} \varepsilon_{\hat{\psi}}, \end{aligned}$$

with $\hat{\psi}(Ng) = \psi(g)$. Since the norm is surjective we can proceed as above.

Chapter 2

Even characters and the ideal class group

2.1 Introduction

In the previous chapter the odd components were treated, this chapter deals with the even components. It will be proved that if K is an Abelian number field and $K \subset \mathbf{Q}(\zeta_{\mathrm{cond}(K)})$ with $p \nmid \phi(\mathrm{cond}(K))$, then the number of elements of an even χ component of the ideal class group equals the number of elements of a χ component of the global units modulo the cyclotomic units. The main ingredient for the proof is theorem 4.1 of Rubin (see [Ru1]). For some characters of a cyclotomic field a generator of the corresponding eigenspace will be given. This makes it possible to do explicit computations.

2.2 Preliminaries

In this section we will see that the cyclotomic units form an Euler system, and a principal ideal κ_r is constructed out of the cyclotomic units. The following notation will be used. Let $F = \mathbf{Q}(\zeta_d)^+$ and write G for its Galois group $\mathrm{Gal}(F/\mathbf{Q})$. Let S be the set of positive square free integers

which are only divisible by primes l such that $l \bmod M = 1$ and l splits completely in F where M is a power of a fixed odd prime p. For every $r \in S$ write $G_r = \mathrm{Gal}(F(\mu_r)/F)$.
As before $N_r = \sum_{\tau \in G_r} \tau$ and $D_l = \sum_{i=1}^{l-2} i\sigma_l^i \in \mathbf{Z}[G_l]$.

Definition 2.1 *The* cyclotomic units *of F are defined by taking the intersection with the global units of F and the group generated by* $\{\pm\zeta_d,\ 1-\zeta_d^a \mid\ 1 < a \leq d-1\}$.

Theorem 2.1 *Write E for the global units and h for the class number of F. Then*

$$[E : C] = 2^b h,$$

where $b = 0$ if $g = 1$ and $b = 2^{g-2} + 1 - g$ if $g \geq 2$, and g is the number of distinct prime factors of d.

Proof. See [Sil].

For $r \in S$ define

$$\xi_r = (\zeta_d \prod_{l|r} \zeta_l - 1)(\zeta_d^{-1} \prod_{l|r} \zeta_l - 1).$$

These cyclotomic units form an (universal) Euler system (see chapter 1) since they satisfy:

i). $\xi_r \in F(\zeta_r)^*$,

ii). $N_l \xi_r = (Fr_l - 1)\xi_{r/l}$.

For the proof of (ii) use

$$\prod_{i=0}^{l-1} (x - \zeta_l^i \beta) = x^l - \beta^l.$$

From these cyclotomic units, a principal ideal in F (modulo M-th powers of ideals) is constructed in the following way.

Lemma 2.1 *For every $r \in S$ there is a $\kappa_r \in F^*/F^{*M}$, such that*

$$\kappa_r \equiv D_r\xi_r \ mod\ (F(\mu_r)^{*M}).$$

Proof. We have an exact sequence

$$0 \to F^* \to F^* \to F^*/F^{*M} \to 0,$$

also

$$0 \to (F'^*)^{G_r} \to (F'^*)^{G_r} \to (F'^*/F'^{*M})^{G_r} \to H^1(F'/F, F'^*),$$

where $F' = F(\mu_r)$. This gives us using Hilbert 90

$$F^*/F^{*M} \cong (F(\mu_r)^*/F(\mu_r)^{*M})^{G_r}.$$

Use this isomorphism and the fact that

$$D_r\xi_r \in (F(\mu_r)^*/F(\mu_r)^{*M})^{G_r},$$

which can be proved using induction on the number of primes dividing r ([Rul]).

2.3 Notation and definitions

From now on we fix the following notation.

p is an odd prime number and M is a large power of p.

$F = \mathbf{Q}(\zeta_d)^+$, where d is a positive integer such that $p \nmid \phi(d)$.

E denotes the global units of F and E_M are the global units of F modulo E^M.

C_M are the cyclotomic units of F modulo E^M.

$G = \mathrm{Gal}(F/\mathbf{Q})$, $\chi \in \hat{G}$.

$O = \mathbf{Z}_p[\zeta_{\phi(d)}] \subseteq \mathbf{Q}_p(\zeta_{\phi(d)})$.

Ξ denotes an irreducible $\mathbf{Z}_p$ representation of G.

Unless specified otherwise $\otimes$ is taken over $\mathbf{Z}_p$.

Definition 2.2 *Let M be a $\mathbf{Z}_p[G]$ module, then $O \otimes M$ is an $O[G]$ module by defining $\sigma(x \otimes m) = x \otimes \sigma m$.*

Lemma 2.2 *Write $\Xi = \sum \rho_i$. Decompose*

$$(O \otimes M)_\Xi = \oplus_i (O \otimes M)_{\rho_i}.$$

Then the $(O \otimes M)_{\rho_i}$ are isomorphic.

Proof. As we saw in lemma 1.7

$$\varepsilon_\Xi = \sum \varepsilon_{\rho_i}.$$

Let $\sigma \in \mathrm{Gal}\mathbf{Q}_p(\zeta_{\phi(d)})/\mathbf{Q}_p)$. Then $\sigma(\varepsilon_\Xi) = \varepsilon_\Xi$ and $\sigma(\varepsilon_{\rho_i}) = \varepsilon_{\rho_i^\sigma}$.
Furthermore σ permutes the ε_{ρ_i} in a transitive way.
Suppose σ does not permute the ε_{ρ_i} in a transitive way, then

$$\varepsilon_\Xi = \sum_k \varepsilon_{\rho_{ik}} + \sum_k \varepsilon_{\rho_{jk}},$$

with the $\varepsilon_{\rho_{ik}}$ in one orbit for all k. This implies that

$$\sigma(\sum_k \varepsilon_{\rho_{ik}}) = \sum_k \varepsilon_{\rho_{ik}}.$$

In other words $\sum_k \rho_{ik}$ is a character with values in $\mathbf{Z}_p$. This is in contradiction with the assumption that Ξ is irreducible over $\mathbf{Z}_p$.

Let the action of $\sigma \in \mathrm{Gal}\mathbf{Q}_p(\zeta_{\phi(d)})/\mathbf{Q}_p)$ on $O \otimes M$ be given by

$$\sigma(x \otimes m) = x^\sigma \otimes m.$$

For every $\sigma \in \mathrm{Gal}\mathbf{Q}_p(\zeta_{\phi(d)})/\mathbf{Q}_p)$ there is an isomorphism

$$(O \otimes M)_{\rho_i} \cong (O \otimes M)_{\rho_i^\sigma}.$$

Since σ acts transitively, they are all isomorphic. This finishes the proof.

In the next section we will see that κ_1 generates some eigenspaces of the cyclotomic units. For these spaces we can use the following theorem of Rubin ([Ru1 th. 4.1]).

Theorem 2.2 *Let Ξ be an irreducible $\mathbf{Z}_p$ representation of $G = Gal(F/\mathbf{Q})$ such that $(C_M)_\Xi$ is generated by $(\kappa_1)_\Xi$ as $(\mathbf{Z}_p[G])_\Xi$ module. Write A for the p-part of the ideal class group of F. Then*

$$\#A_\Xi | \#(E_M/C_M)_\Xi.$$

Proof. See [Rul]. Note that if $(C_M)_\Xi$ is generated by $(\kappa_1)_\Xi$ as $(\mathbf{Z}_p[G])_\Xi$ module, then (using the notation of the proof)

$$\#(E_M/C_M)_\Xi = t_1^{\dim \Xi},$$

since $\mathbf{Z}_p[G]_\Xi$ is a free $\mathbf{Z}_p$ module of rank $\dim \Xi$.

2.4 The units

Lemma 2.3 *Let χ be a non trivial character of G, then $(O \otimes E_M)_\chi$ is a cyclic O module.*

Proof. $E_{tors} = \pm 1$. The Dirichlet Unit Theorem gives us E/E_{tors} is free of rank $(\frac{\phi(d)}{2} - 1)$ which implies

$$E_M \cong \oplus_{(\phi(d)/2)-1} \mathbf{Z}/M\mathbf{Z}.$$

Also

$$O \otimes E_M \cong \oplus_\chi (O \otimes E_M)_\chi.$$

If χ is the trivial character then $(O \otimes E_M)_\chi$ does not contribute since

$$\epsilon_1(x \otimes y) = x \otimes Ny = x \otimes 1.$$

In a similar way as in [G] it can be proved that for χ a non trivial character

$$\dim_{O/pO}(O \otimes E_p)_\chi = 1.$$

Thus $(O \otimes E_M)_\chi$ is not trivial for every character $\chi \neq 1$.

This results in

$$(O \otimes E_M)_\chi \cong O \otimes \mathbf{Z}/M\mathbf{Z},$$

since both decompositions have the same number of components.

Corollary 2.1 *i). $(O \otimes C_M)_\chi$ is a cyclic O module,*

ii). $(E_M)_\Xi$ and $(C_M)_\Xi$ are cyclic $\mathbf{Z}_p[G]_\Xi$ modules.

Proof. Since E_M/C_M is finite we have (i). $(E_M)_\Xi$ is cyclic because any linear component has rank one (they are all isomorphic) and in the same way as in (i) this implies that $(C_M)_\Xi$ is cyclic.

Proposition 2.1 *We have for all the characters of $\widehat{Gal(F/\mathbf{Q})}$ of conductor d that $(O \otimes C_M)_\chi$ is generated by $(1 \otimes \kappa_1)_\chi$, where* $\kappa_1 = (1 - \zeta_d)(1 - \zeta_d^{-1})$.

Proof. Write $d = q_1^{n_1} ... q_l^{n_l}$. In F we have the following generators for the cyclotomic units:

i)
$$(1 - \zeta_{\prod q_j^{m_j}})(1 - \zeta_{\prod q_j^{m_j}}^{-1})$$

with at least one $m_j = 0$,

ii)
$$(1 - \zeta_{\prod_{j=1}^{l} q_j^{m_j}})(1 - \zeta_{\prod_{j=1}^{l} q_j^{m_j}}^{-1})$$

and none of the m_j's are zero.

The units under i) belong to subfields of F and they do not contribute to $(O \otimes C_M)_\chi$.

This can be derived as follows: suppose the $m_1, ..., m_i$ in i) are zero.

Write $a = q_1^{n_1} ... q_i^{n_i}, b = q_{i+1}^{m_{i+1}} ... q_l^{m_l}$. Using the isomorphism

$$\mathrm{Gal}(\mathbf{Q}(\zeta_d)/\mathbf{Q}) \cong \mathrm{Gal}(\mathbf{Q}(\zeta_a)/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{Q}(\zeta_{d/a})/\mathbf{Q})$$

we can decompose χ_d as $\chi_a \cdot \chi_{\frac{d}{a}}$.

$$
\begin{aligned}
(1 \otimes (1-\zeta_b)(1-\zeta_b^{-1}))_\chi &= \\
\frac{1}{|G^+|} \sum_{\sigma \in G^+} \chi(\sigma) \otimes (1-\zeta_b)(1-\zeta_b^{-1})^{\sigma^{-1}} &= \\
\frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma) \otimes (1-\zeta_b)(1-\zeta_b^{-1})^{\sigma^{-1}} &= \\
\frac{1}{|G|} \sum_{\sigma_1} \chi_a(\sigma_1) \sum_{\sigma_2} \chi_{\frac{d}{a}}(\sigma_2) \otimes (1-\zeta_b)(1-\zeta_b^{-1})^{\sigma_2^{-1}}, &
\end{aligned}
$$

where $\sigma_1 \in \mathrm{Gal}(\mathbf{Q}(\zeta_a)/\mathbf{Q})$ and $\sigma_2 \in \mathrm{Gal}(\mathbf{Q}(\zeta_{d/a})/\mathbf{Q})$.

Since $\sum_{\sigma_1} \chi_a(\sigma_1) = 0$, the units as mentioned in i) can be neglected.

The units under ii) can be expressed in the generator $(1 \otimes \kappa_1)_\chi$ using the property

$$
1 - \zeta_m^a = \prod_{j=0}^{n/m-1} (1 - \zeta_n^{a+mj}) \text{ for } m \mid n.
$$

Write $\prod_{j=1}^{l} q_j^{m_j} = a$ then

$$
N_{F/\mathbf{Q}(\zeta_a)^+}(\kappa_1) = (1-\zeta_a)(1-\zeta_a^{-1}),
$$

and

$$
(1 \otimes N\kappa_1)_\chi = \sum_{\sigma \in \mathrm{Gal}F/\mathbf{Q}(\zeta_a)^+} \chi(\sigma)(1 \otimes \kappa_1)_\chi.
$$

Remark 2.1 If $d = q^r$ with q prime then the above lemma holds for every non trivial character. The cyclotomic units in $\mathbf{Q}(\zeta_{q^r})^+$ are generated by the units described in (ii), thus $(O \otimes C_M)_\chi$ is generated by $(1 \otimes \kappa_1)_\chi$ for every χ.

Corollary 2.2 *If $\Xi = \sum_i \rho_i$ with $f_{\rho_i} = d$ for all i, then $(C_M)_\Xi$ is generated (as $\mathbf{Z}_p[G]$-module) by $(\kappa_1)_\Xi$. If $d = q^r$ with q prime, then $(C_M)_\Xi$ is generated by $(\kappa_1)_\Xi$ for all irreducible $\mathbf{Z}_p$ representations of G.*

Now we can apply theorem 2.2 for those representations where $(C_M)_\Xi$ is generated by $(\kappa_1)_\Xi$. The other cases are satisfied by induction on the number of primes dividing d.

2.5 An induction argument

Write A for the p-part of the ideal class group of F. Our aim is to proof that for all characters in $\hat{G}$ we have

$$\#(O \otimes A)_\chi = \#(O \otimes E_M/C_M)_\chi.$$

It is sufficient to prove that for all $\mathbf{Z}_p$ irreducible representations Ξ of G we have

$$\#(A)_\Xi = \#(E_M/C_M)_\Xi,$$

since the linear components are isomorphic (see lemma 2.2).

Proposition 2.2 *If $F = \mathbf{Q}(\zeta_{q^r})^+$ then*

$$\#(O \otimes A)_{\rho_i} = \#(O \otimes E_M/C_M)_{\rho_i}$$

for all linear characters of $Gal(F/\mathbf{Q})$.

Proof. We know that $(C_M)_\Xi$ is generated by $(\kappa_1)_\Xi$ for all irreducible $\mathbf{Z}_p$ representations of G. Thus using theorem 2.2 we have

$$\#A_\Xi \mid \#(E_M/C_M)_\Xi.$$

The class number formula (theorem 2.1) gives

$$\#A_\Xi = \#(E_M/C_M)_\Xi.$$

In the same way we obtain

Lemma 2.4 *If d is divisible by more than one prime and $\Xi = \sum_i \rho_i$ with $f_{\rho_i} = d$ for all i, then*

$$\#A_\Xi \mid \#(E_M/C_M)_\Xi.$$

Now we are ready for the induction argument.

Theorem 2.3 *Let $F = \mathbf{Q}(\zeta_d)^+$ and $p \nmid \phi(d)$. Then for all irreducible $\mathbf{Z}_p$ representations of $G = Gal(F/\mathbf{Q})$*

$$\#A_\Xi = \#(E_M/C_M)_\Xi.$$

Proof. Write $d = q_1^{n_1} \dots q_l^{n_l}$. For $K = \mathbf{Q}(\zeta_{q_i^{n_i}})^+$ we already know that

$$\#A_\Xi = \#(E_M/C_M)_\Xi,$$

where Ξ is an irreducible $\mathbf{Z}_p$ representation of $\mathrm{Gal}(\mathbf{Q}(\zeta_{q_i^{n_i}})^+/\mathbf{Q})$.

Suppose we have for all $K = \mathbf{Q}(\zeta_{q_1^{n_1}} \dots \zeta_{q_j^{n_j}})^+$ with $j \leq l-1$ and for all irreducible $\mathbf{Z}_p$ representations of $\mathrm{Gal}(K/\mathbf{Q}) = G/N$

$$\#(A_K)_\Xi = \#(E_{K_M}/C_{K_M})_\Xi.$$

If we take an arbitrary irreducible $\mathbf{Z}_p$ representations of G we have the following two possibilities:

i). $\Xi = \sum \rho_i$ with $f_{\rho_i} = d$ for all i,

ii). Ξ is an irreducible representation of a cyclotomic subfield.

In case (i) apply lemma 2.4. This gives

$$\#A_\Xi | \#(E_M/C_M)_\Xi.$$

In case (ii) we have $N \subseteq \ker \Xi$ for a normal subgroup N of G, since Ξ is an irreducible $\mathbf{Z}_p$ representation of G/N if and only if Ξ is an irreducible $\mathbf{Z}_p$ representation of G with $N \subseteq \ker \Xi$.

Write $G/N = \mathrm{Gal}(\mathbf{Q}(\zeta_{q_1^{n_1} \dots q_j^{n_j}})^+/\mathbf{Q})$ and $N = \mathrm{Gal}(F/K)$.

Then

$$\varepsilon_\Xi = \frac{1}{|N|} N_{F/K} \varepsilon_{\hat{\Xi}} \text{ with } \hat{\Xi}(Ng) = \Xi(g).$$

Using

$$E_{K_M}/C_{K_M} \to E_{F_M}/C_{F_M} \to E_{K_M}/C_{K_M}$$

which sends an element x to $x^{[F:K]}$, we have

$N_{F/K}(E_{F_M}/C_{F_M}) = (E_{K_M}/C_{K_M})$ and in the same way $N_{F/K}A_F = A_K$, since $p \nmid [F:K]$. So

$$\#(A_F)_\Xi = \#(A_K)_{\hat{\Xi}} = \#(E_{K_M}/C_{K_M})_{\hat{\Xi}} = \#(E_{F_M}/C_{F_M})_\Xi.$$

This gives for all irreducible $\mathbf{Z}_p$ representations of G

$$\#A_\Xi | \#(E_M/C_M)_\Xi.$$

From the class number formula it follows that the numbers of elements are equal.

Just as in chapter 1, we can extend the results on the cyclotomic fields to an arbitrary Abelian field K, with $p \nmid$ cond (K).

2.6 K real Abelian

Let K be a real Abelian field such that $p \nmid \text{cond}\,(K)$. Write $F = \mathbf{Q}(\zeta_{\text{cond}\,(K)})^+$ and let χ be a character of G such that $\text{Gal}(F/K) \subseteq \ker \chi$.

Write $G = \oplus_i \sigma_i N$ with $\sigma_i \in G/N$. Then

$$\begin{aligned} \varepsilon_\chi &= \frac{1}{G} N_{F/K} \Big(\sum_{\sigma_i \in G/N} \chi(\sigma_i N) \sigma_i^{-1} \Big) \\ &= \frac{N}{G} N_{F/K} \varepsilon_{\hat{\chi}}, \end{aligned}$$

with $\hat{\chi}(Ng) = \chi(g)$.

Since the norm is surjective we get

$$\#(O \otimes A_K)_{\hat{\chi}} = \#(O \otimes (E_K)_M/(C_K)_M)_{\hat{\chi}}.$$

In the next section I will give, following Washington (see [W]), a criterion for computing $(E_M/C_M)_\Xi$.

2.7 When is $(E_M/C_M)_\Xi$ trivial?

Let Ξ be an irreducible $\mathbf{Z}_p$ representation of $G = \mathrm{Gal}(\mathbf{Q}(\zeta_d)^+/\mathbf{Q})$ with $p \nmid \phi(d)$ such that $(\kappa_1)_\Xi$ generates $(C_M)_\Xi$. Then

$(E_M/C_M)_\Xi$ non trivial $\Leftrightarrow$ $(\kappa_1)_\Xi$ is a p-th power of a unit of $\mathbf{Q}(\zeta_d)^+$.

Proposition 2.3 *If $p \mid d$, write $b = \frac{d}{p}$, take a prime l such that $l \equiv 1$ mod d and k such that $l = kd + 1$. Let t be an integer such that $(t, l) = 1$, $t^{kb} \not\equiv 1$ mod l and let λ be a prime of $\mathbf{Q}(\zeta_d)$ above l such that $t^k \equiv \zeta_d$ mod λ. Define*

$$Q = \prod_{(a,d)=1} (1 - t^{ak})^{\Xi(\sigma_a^{-1})}.$$

Then

$$(\kappa_1)_\Xi \text{ is a } p\text{-th power mod } \lambda \Leftrightarrow Q^{kb} \equiv 1 \text{ mod } l.$$

Proof. Since $t^{kb} \not\equiv 1 \bmod l$ and $t^{kd} \equiv 1 \bmod l$ it follows that t^k is a d-th root of unity mod λ. Since l splits completely in $\mathbf{Q}(\zeta_d)$ we know that the primes above l are of the form $(l, a - \zeta_d)$, where a mod l is of order d, so there exists a prime λ above l such that $t^k \equiv \zeta_d \bmod \lambda$. Since l splits

completely we have that $\mathbf{Z}[\zeta_d]/\lambda$ is cyclic of order $l-1=kd$. From this follows

$$Q^{kb} \equiv 1 \bmod l \leftrightarrow Q \text{ is a } p\text{-th power mod } \lambda.$$

Since

$$(\kappa_1)_{\Xi}^{\phi(d)/2} = \prod_{(a,d)=1} (1-\zeta_d^a)^{\Xi(\sigma_a-1)},$$

we have

$$(\kappa_1)_{\Xi}^{\phi(d)/2} \equiv Q \bmod \lambda,$$

and

$$(\kappa_1)_{\Xi}^{\phi(d)/2} \text{ is a } p\text{-th power } \Leftrightarrow (\kappa_1)_{\Xi} \text{ is a } p\text{-th power.}$$

Remark 2.2 If $\Xi = \sum \rho_i$ with $f_{\rho_i} = m$, for all i, then there is a field $K = \mathbf{Q}(\zeta_m)$ such that

$$\#(E_{K_M}/C_{K_M})_{\hat{\Xi}} = \#(E_{F_M}/C_{F_M})_{\Xi}$$

and $\hat{\Xi} = \sum \psi_i$ with $f_{\psi_i} = m$.

In this way we can also compute $(E_{F_M}/C_{F_M})_{\Xi}$ if Ξ belongs to a cyclotomic subfield of F. Of course the same can be done for K real Abelian with $p \nmid \phi(\text{cond })(K)$.

In chapter 3 I will use this to investigate the structure of the tame kernel of some quadratic number fields.

Chapter 3

Applications to K-theory

3.1 Introduction

For F an Abelian number field and p an odd prime, which is unramified in F and does not divide the degree $[F : \mathbf{Q}]$, it will be showed that the p-rank of the K_2 of the ring of integers of F equals the p-rank of an eigenspace of the ideal class group of $F(\zeta_p)$. In this way we can apply the results of the preceding chapters to compute the p-rank of the tame kernel. Also upper and lower bounds of the p-rank of the tame kernel will be given.

Computations are made for the tame kernel of a real quadratic number field and for the tame kernel of the maximal real cyclotomic subfield. For the tame kernel of a real quadratic number field we find that with the exception of a few unsolved cases the p-rank of the K_2 of the ring of integers of a real quadratic number field with discriminant less than 20000 is always cyclic, where p is an odd prime such that $p \nmid \mathrm{disc}(F)\phi(\mathrm{cond}(F(\zeta_p)))$. Under certain restrictions the condition $p \nmid \mathrm{disc}(F)$ can be removed. I cannot prove that the p-rank of the tame kernel of a real quadratic number field is always cyclic. Such a proof would imply that the eigenspace of the corresponding ideal class group is also always cyclic. J. Browkin told me recently that for $p = 5$ a counter

example can be constructed. A possible candidate will be given using work of [Mes].

3.2 Preliminaries

In this section I introduce some facts which will be needed in the sequel. K-theory is discussed separately in the next section. All the material of this section can be found in [W].

Definition 3.1 *Let χ be a Dirichlet character of conductor f. The* L-series *attached to χ is defined by*

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},\ Re(s) > 1.$$

$L(s,\chi)$ may be continued analytically to the whole complex plane, except for a simple pole at $s = 1$ when $\chi = 1$.

Definition 3.2 *For K a number field and O_K its ring of integers, the* Dedekind zeta *function is defined by*

$$\zeta_K(s) = \sum_{\mathfrak{a} \text{ ideal} \neq 0,\ \mathfrak{a} \subseteq O_K} \frac{1}{N(\mathfrak{a})^s},\ Re(s) > 1.$$

$\zeta_K(s)$ may be continued analytically to the whole complex plane, except for a simple pole at $s = 1$.

Theorem 3.1 *Let K be an Abelian number field, X the character group of K, and $\zeta_K(s)$ the Dedekind zeta function of K. Then*

$$\zeta_K(s) = \prod_{\chi \in X} L(s,\chi).$$

Since

$$L(1-n,\chi) = \frac{-B_{n,\chi}}{n} \text{ for } n \geq 1,$$

we obtain

$$\zeta_K(-1) = \prod_{\chi \in X} -\frac{B_{2,\chi}}{2}.$$

Lemma 3.1 *Let χ be an even character such that $p^2 \nmid f_\chi$. Then*

$$B_{1,\omega\chi} \equiv \frac{B_{2,\chi}}{2} \ mod\ p.$$

For the proof of this lemma we need two properties of the p-adic L-functions, namely:

i). Let χ be a Dirichlet character. Then there exists a p-adic meromorphic (analytic if $\chi \neq 1$) function $L_p(s,\chi)$ on $\{s \in \mathbf{C}_p \mid \ \mid s \mid < p^{-1/(p-1)}\}$ such that

$$L_p(1-n,\chi) = -(1-\chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n},\ n \geq 1,$$

ii). Suppose $\chi \neq 1$, $p^2 \nmid f_\chi$. Let $m, n \in \mathbf{Z}$. Then

$$L_p(m,\chi) \equiv L_p(n,\chi) \bmod p.$$

Property (i) gives us:

$$L_p(0,\omega^2\chi) = -B_{1,\omega\chi},$$

$$L_p(-1,\omega^2\chi) = -B_{2,\chi}/2.$$

Now use (ii).

3.3 Facts about K_2

Let R be a commutative ring. Let $e_{ij}^\lambda \in GL(n,R)$ denote the elementary matrix with entry λ in the (i,j)-th place, where $\lambda \in R$. The *Steinberg group*, defined below, imitates the behaviour of elementary matrices.

Definition 3.3 *Let R be a commutative ring. For $n \geq 3$ the* Steinberg group *$St(n,R)$ is defined by generators x_{ij}^λ subject to the relations:*

i). $x_{ij}^{\lambda} x_{ij}^{\mu} = x_{ij}^{\lambda+\mu}$,

ii). $[x_{ij}^{\lambda}, x_{jl}^{\mu}] = x_{il}^{\lambda\mu}$ *for* $i \neq l$,

iii). $[x_{ij}^{\lambda}, x_{kl}^{\mu}] = 1$ *for* $j \neq k, i \neq l$.

We have a homomorphism

$$\phi : St(n, R) \to Gl(n, R)$$

defined by $\phi(x_{ij}^{\lambda}) = e_{ij}^{\lambda}$. Passing to the direct limit we obtain corresponding groups and a corresponding homomorphism:

$$\phi : St(R) \to GL(R).$$

Definition 3.4 *The kernel of the homomorphism* $\phi : St(R) \to GL(R)$ *will be called* K_2R.

Proposition 3.1 *The group* K_2R *is the center of the Steinberg group* $St(R)$.

Proof. See [Mi].

Definition 3.5 *Let* F *be a field and* A *an Abelian group. A* Steinberg symbol *on* F *is a bimultiplicative symbol* $c(x, y)$ *with* $c : F^* \times F^* \to A$ *satisfying* $c(x, 1 - x) = 1$.

Theorem 3.2 *The Abelian group* $K_2(F)$ *has a presentation, in terms of generators and relations, as follows. The given generators* $\{x, y\}$, *with* $x, y \in F^*$, *are subject only to the following relations and their consequences:*

i). $\{x, 1 - x\} = 1$ *for* $x \neq 0, 1$,

ii). $\{xz, y\} = \{x, y\}\{z, y\}$,

iii). $\{x, zy\} = \{x, z\}\{x, y\}$.

This theorem is due to Matsumoto. For a proof see ([Mi]).
The theorem of Matsumoto states that $(x,y) \mapsto \{x,y\} \in K_2(F)$ is the universal Steinberg symbol on a field F.

Lemma 3.2 *If F is a finite field, then $\{x,y\} = 1$ for all x and y.*

Proof. See [Mi].

Lemma 3.3 *Suppose v is a discrete valuation on F and let $\mathfrak{p}$ be the maximal ideal of the valuation ring of v, then*

$$d_v(x,y) = (-1)^{v(x)v(y)} x^{v(y)}/y^{v(x)} \ mod\ \mathfrak{p}$$

defines a Steinberg symbol d_v on F^* with values in k_v^*.

Proof. See [Mi].

The symbol d_v is called the tame symbol. For each finite prime $\mathfrak{p}$ it induces a map

$$\tau_{\mathfrak{p}} : K_2(F) \to k_{\mathfrak{p}}^*.$$

Together they give a surjective homomorphism (see[Mi])

$$\tau : K_2(F) \to \bigoplus_{\mathfrak{p}} k_{\mathfrak{p}}^*.$$

The kernel of τ is called the *tame kernel.*

Theorem 3.3 *For the ring of integers O_F of F the tame kernel coincides with $K_2(O_F)$.*

Proof. Let R be a Dedekind domain, $\mathfrak{p}$ a maximal ideal of R, and F its quotient field. Then there exist a long exact sequence

$$\cdots \to \bigoplus_{\mathfrak{p}} K_2(k_{\mathfrak{p}}) \to K_2(R) \to K_2(F) \xrightarrow{\tau} \bigoplus_{\mathfrak{p}} k_{\mathfrak{p}}^* \to \cdots$$

For F a number field one has from lemma 3.2 $K_2(k_\mathfrak{p}) = 0$. Moreover, τ is surjective. Thus we obtain the short exact sequence

$$0 \to K_2(O_F) \to K_2(F) \to \bigoplus_{\mathfrak{p}} k_\mathfrak{p}^* \to 0.$$

Theorem 3.4 *The tame kernel $K_2(O_F)$ is a finite Abelian group.*

Proof. Obviously the group is Abelian since it is the center of the Steinberg group. For the proof of finiteness see [Ga].

Theorem 3.5 *Let F be a totally real number field and p an odd prime. Then the p-part of $\#K_2(O_F)$ equals the p-part of $w_2(F)\zeta_F(-1)$, where $w_2(F)$ is defined as the largest integer n such that $Gal(F(\zeta_n)/F)$ has exponent 2.*

Proof. See [Wi].

Lemma 3.4 *Let F be a number field and p a prime such that $p \nmid 6\ disc(F)$. Then the p-primary part of $w_2(F)$ is trivial. For $F = \mathbf{Q}(\zeta_n)$, we have $w_2(F) = w_2(F^+) = lcm(24, 2n)$.*

Proof. (See [L-M]) The p-primary part of $w_2(F)$ is p^n, where n is the largest integer for which $\mathrm{Gal}(F(\zeta_{p^n})/F)$ has exponent 2. Now if $p \nmid \mathrm{disc}(F)$, then $[F(\zeta_{p^n}) : F] = p^{n-1}(p-1)$. So for $p = 2$ we have $n = 3$, and for $p = 3$ we have $n = 1$. If $F = \mathbf{Q}(\zeta_n)$ and $p^r \mid n$, $p^{r+1} \nmid n$ then $[F(\zeta_{p^n}) : F] = p^{n-r}$. This gives $w_2(F) = \mathrm{lcm}(24, 2n)$.

Definition 3.6 *Define $\lambda_\mathfrak{p}$ as the homomorphism induced by the Hilbert symbol $(\ ,\ /\mathfrak{p})_2$, where $\mathfrak{p}$ is real infinite. Then $\lambda_\mathfrak{p}$ induces a surjective homomorphism (see [K]):*

$$K_2(O_F) \to \bigoplus_{\mathfrak{p}\ real\ infinite} \mu_2.$$

Now $K_2^+(O_F)$ is defined as the kernel of the above homomorphism.

3.4 Some exact sequences

We have the following exact sequence which relates the tame kernel to an ideal class group (See [K]).

Theorem 3.6 *Let $n = p^r$, $n \geq 3$ with p prime and r a positive integer. For F a number field, with $\zeta_n \in F$, we have*

$$0 \to \mu_n \otimes Cl(O_F[\tfrac{1}{p}]) \to K_2^+(O_F)/n \to \bigoplus_{\mathfrak{p}|p} \mu_n \to \mu_n \to 0.$$

$Cl(O_F[\frac{1}{p}])$ denotes the ideal class group where the primes above p are trivial.
For example, if F is the cyclotomic field $\mathbf{Q}(\zeta_p)$ we have

$$K_2(\mathbf{Z}[\zeta_p])/p \cong \mu_p \otimes Cl(\mathbf{Z}[\zeta_p]),$$

since the prime above p is trivial in $Cl(\mathbf{Z}[\zeta_p])$.

If F does not contain a primitive p-th root of unity, we have the following relation (See [K]).

Theorem 3.7 *Let p be an odd prime, F a number field and ζ_p a primitive p-th root of unity. Suppose $\zeta_p \notin F$, then*

$$0 \to (\mu_p \otimes Cl(O_{F(\zeta_p)}[\tfrac{1}{p}]))^\Gamma \to K_2O_F/p \to \bigoplus_{\mathfrak{p} \in S'} \mu_p \to 0.$$

Here $\Gamma = Gal(F(\zeta_p)/F)$ and S' is the set of p-adic primes of F which split completely in $F(\zeta_p)$.

For example, if the ramification index of p in F is less than $p-1$, we have an isomorphism

$$(\mu_p \otimes Cl(O_{F(\zeta_p)}[\tfrac{1}{p}]))^\Gamma \cong K_2O_F/p,$$

since S' is empty due to complete ramification of p in $\mathbf{Q}(\zeta_p)$.

If F is Abelian and p does not ramify in F, we can simplify even more.

3.5 F Abelian

From now on the following notation will be used. Fix an odd prime p such that $p \nmid \mathrm{disc}(F)[F:\mathbf{Q}]$. Let $K = F(\zeta_p)$ and write O_K for its ring of integers. Let $\Gamma = \mathrm{Gal}(K/F)$ be as before and write G for $\mathrm{Gal}(K/\mathbf{Q})$. If n is the exponent of G, define $O = \mathbf{Z}_p[\zeta_n]$. Write A for the p-part of the ideal class group of K.
If we view ε_{ω^i} as an element of $O[G]$, we get for H a $\mathbf{Z}_p[G]$ module

$$O \otimes_{\mathbf{Z}_p} (H)_{\omega^i} \cong \bigoplus_{\chi \in \widehat{\mathrm{Gal}(F/\mathbf{Q})}} (O \otimes_{\mathbf{Z}_p} H)_{\omega^i\chi}.$$

This can be proved by using $\sum_{\chi \in \widehat{\mathrm{Gal}(F/\mathbf{Q})}} \varepsilon_\chi = 1$.

Lemma 3.5 *Let W be the subgroup of $Cl(O_{F(\zeta_p)})$ generated by the primes above p, then $(\mu_p \otimes W)^\Gamma \cong (W/W^p)_{\omega^{-1}}$.*

Proof.

$$\begin{aligned}
(\mu_p \otimes W)^\Gamma &\cong (\mu_p \otimes W/W^p)^\Gamma \\
&= \{\zeta \otimes \bar{x} \mid \zeta^\sigma \otimes \bar{x}^\sigma = \zeta \otimes \bar{x},\ \forall\, \sigma \in \Gamma\} \\
&= \{\zeta \otimes \bar{x} \mid \zeta^{\omega(\sigma)} \otimes \bar{x}^\sigma = \zeta \otimes \bar{x},\ \forall\, \sigma \in \Gamma\} \\
&= \{\zeta \otimes \bar{x} \mid \zeta \otimes \bar{x}^\sigma = \zeta \otimes \bar{x}^{\omega^{-1}(\sigma)},\ \forall\, \sigma \in \Gamma\} \\
&\cong \{\bar{x} \mid \bar{x}^\sigma = \bar{x}^{\omega^{-1}(\sigma)},\ \forall\, \sigma \in \Gamma\} \\
&= (W/W^p)_{\omega^{-1}}.
\end{aligned}$$

In exactly the same way it can be proved (see [G]), that

$$(\mu_p \otimes Cl(O_{F(\zeta_p)})^\Gamma \cong (A/(A)^p)_{\omega^{-1}}.$$

In combination with the following proposition we obtain that the p-rank of $K_2(O_F)$ equals the p-rank of an eigenspace of the p-part of $Cl(O_{F(\zeta_p)})$.

Proposition 3.2 *We have an isomorphism*

$$(\mu_p \otimes Cl(O_K))^\Gamma \cong (\mu_p \otimes Cl(O_K[\tfrac{1}{p}]))^\Gamma.$$

Proof. Consider the exact sequence

$$0 \to W \to Cl(O_{F(\zeta_p)}) \to Cl(O_{F(\zeta_p)}[\tfrac{1}{p}]) \to 0,$$

where W is the subgroup of $Cl(O_K)$ generated by the primes above p. Taking the tensor product and Galois invariants we obtain the exact sequence

$$(\mu_p \otimes W)^\Gamma \to (\mu_p \otimes Cl(O_K))^\Gamma \to (\mu_p \otimes Cl(O_K[\tfrac{1}{p}]))^\Gamma \to 0.$$

Use the isomorphism $(\mu_p \otimes W)^\Gamma \cong (W/W^p)_{\omega^{-1}}$. By definition we have for a generator P of $(W/W^p)_{\omega^{-1}}$ that $P^\sigma = P^{\omega^{-1}(\sigma)}$ for all $\sigma \in \Gamma$. Also the primes above p in F are completely ramified in K, since $p \nmid \mathrm{disc}(F)$. So every generator P of $(W/W^p)_{\omega^{-1}}$ is fixed for all $\sigma \in \Gamma$. In other words, $(\mu_p \otimes W)^\Gamma$ is trivial because P lies in two different eigenspaces which are disjoint.

This gives us:

Proposition 3.3 *i).* $(A/A^p)_{\omega^{-1}} \cong K_2O_F/p$,

ii). $A_{\omega^{-1}}$ *cyclic* $\Leftrightarrow K_2O_F\{p\}$ *cyclic,*

iii). If $p \nmid \phi(cond\ (F(\zeta_p)))$, *then*

$$\#(E_M^+/C_M^+)_{\omega^{-1}} \equiv \#K_2O_F^-\{p\} \ mod\ p.$$

Proof. For the proof decompose $K_2O_F\{p\}$ as $K_2O_{F^+}\{p\} \oplus K_2O_F^-\{p\}$. Using the results of chapter 1 and 2 we have

$$\#(A)_{\omega^{-1}} = p^{\sum_{\chi \text{ even}} \mathrm{ord}_p B_{1,\omega\chi^{-1}}} \cdot \#(E_M^+/C_M^+)_{\omega^{-1}}.$$

In particular if F is real we have $\#(A)^-_{\omega^{-1}} = p^{\sum_{\chi \text{ even}} \mathrm{ord}_p B_{1,\omega\chi^{-1}}}$ and (using(i))

$$\#K_2O_{F^+}\{p\} \equiv \#(A)^-_{\omega^{-1}} \bmod p.$$

Thus

$$\#(E_M^+/C_M^+)_{\omega^{-1}} = \#(A)^+_{\omega^{-1}} \equiv \#K_2O_F^-\{p\} \bmod p.$$

We can make upper and lower bounds for the p-rank of the tame kernel. For F real these bounds are more exact than for F complex. I am unable to compute the number of elements of an eigenspace of the units modulo the cyclotomic units, so an upper bound for F complex has to be given with Bernoulli numbers. The idea behind using Bernoulli numbers for the even components is the reflection principle, which relates an odd and an even component in the following way (see [G]).

Write a_ψ for the p-rank of A_ψ. If χ is even, then

$$0 \leq a_{\omega^{-1}\chi^{-1}} - a_{\omega^2\chi} \leq 1.$$

If χ is odd, then

$$0 \leq a_{\omega^2\chi} - a_{\omega^{-1}\chi^{-1}} \leq 1.$$

Corollary 3.1 *For F a totally real Abelian field with p as above*

$$n \leq p\text{-}rk\ K_2(O_F) \leq \sum_{\chi\ even} ord_p B_{1,\omega\chi^{-1}},$$

where n is the number of $\chi \in Gal(F/\mathbf{Q})$ such that $ord_p B_{1,\omega\chi^{-1}} \neq 0$. For F not totally real

$$m + n \leq p\text{-}rk\ K_2(O_F) \leq \sum_{\chi\ odd} ord_p B_{1,\omega^2\chi} + \sum_{\chi\ even} ord_p B_{1,\omega\chi^{-1}},$$

where m is the number of $\chi \in Gal(F/\mathbf{Q})$ such that $(\kappa_1)_{\omega^{-1}\chi^{-1}}$ is a p-th power in $\mathbf{Q}(\zeta_p, \zeta_{cond\ (F)})$.

In the next section I will apply these results to compute the structure of the tame kernel of a real quadratic field. Browkin gave me a list of all unsolved structures of the tame kernel where F has discriminant less than 20000. Most of them are cyclic, but there remain a few cases which I am unable to solve.

3.6 The tame kernel of a real quadratic number field

Let F be real quadratic, write O_F for its ring of integers and let p be a prime with $p \nmid 6\,\mathrm{disc}(F)\phi(\mathrm{cond}(F(\zeta_p)))$. Let χ be the quadratic character of F. As we have seen

$$\#A_{\omega^{-1}} = p^{\mathrm{ord}_p B_{1,\omega} + \mathrm{ord}_p B_{1,\omega\chi}}$$

and

$$B_{1,\omega\chi^{-1}} \equiv \frac{B_{2,\chi^{-1}}}{2} \bmod p.$$

For $\chi = 1$ we have $B_{2,1} = \frac{1}{6}$, so $B_{1,\omega}$ is not divisible by p for $p \geq 5$. From theorem 3.5 and lemma 3.4 it follows that the p-part of $\#K_2(O_F)$ equals the p-part of $B_{2,\chi}$. If a power of p divides $B_{2,\chi}$, we can use the following lemma.

Lemma 3.6 *Let l be a positive integer equal to $ord_p B_{1,\omega\chi^{-1}}$. Then*

$$0 \leq p\text{-}rank\ K_2O_F \leq n$$

with $n = \ min\{l, ord_p B_{2,\chi}\}$.

This implies

$$\mathrm{ord}_p B_{1,\omega\chi^{-1}} = 1 \Rightarrow K_2O_F\{p\} \text{ cyclic.}$$

Write d_F for the discriminant of F then $f_{\omega\chi^{-1}} = pd_F$. Thus by definition

$$B_{1,\omega\chi^{-1}} = \frac{1}{pd_F} \sum_{a=1}^{pd_F} \omega(a)(\frac{d_F}{a})a,$$

so $p^2 \nmid B_{1,\omega\chi^{-1}}$ is equivalent to

$$p^3 \nmid \sum_{a=1,(a,pd_F)=1}^{pd_F} a^{p^2+1}(\frac{d_F}{a}),$$

since $\omega(a) \equiv a^{p^2} \bmod p^3$.

Note that if we want to examine $p = 3$, we also have to compute $B_{1,\omega}$

Remark 3.1 I assumed that $p \nmid \phi(\mathrm{cond}(F(\zeta_p)))$ but as already mentioned before this also works for $p \nmid [K : \mathbf{Q}]$, where K is an imaginary Abelian extension of $\mathbf{Q}$. If we take $K = \mathbf{Q}(\zeta_p)F$, then the assumption of [M-W] is fulfilled.

Now the cases remain where p^2 divides $B_{1,\omega\chi^{-1}}$. If $p \mid \phi(\mathrm{cond}(F(\zeta_p)))$, we cannot proceed. This gives the following unsolved cases where (d,p) denotes the p-primary part of $K_2(O_F)$ with $d = \mathrm{disc}\ (F)$.

(11861,7)
(6497,11)
(18921,13)

For the other cases we will use the reflection principle.
If we show that $(A)_{\omega^2\chi}$ is trivial, then $(A)_{\omega^{-1}\chi}$ has to be cyclic.

Let $d = \mathrm{disc}(F)$, $L = \mathbf{Q}(\zeta_{pd})$ and $K = F(\zeta_p)$. Then $\omega^2\chi$ is an even primitive character of L, so $(\kappa_1)_{\omega^2\chi}$ generates $(C_{L_M})^+_{\omega^2\chi}$. Also

$$\#(E^+_{L_M}/C^+_{L_M})_{\omega^2\chi} = \#(E^+_{K_M}/C^+_{K_M})_{\omega^2\chi},$$

so

$$(\kappa_1)_{\omega^2\chi} \text{ is not a } p\text{-th power of a unit in } L^+ \Rightarrow (A)_{\omega^{-1}\chi} \text{ cyclic.}$$

A reformulation of $(\kappa_1)_{\omega^2\chi}$ is not a p-th power of a unit in L^+ gives the following lemma (See prop. 2.3).

Lemma 3.7 *Take $l \equiv 1 \bmod pd$, say $l = kpd+1$ and let t be an integer such that $(t,l) = 1$, $t^{kd} \not\equiv 1 \bmod l$. Let λ be a prime of $\mathbf{Q}(\zeta_{pd})$ above l such that $t^k \equiv \zeta_{pd} \bmod \lambda$. Define*

$$Q = \prod_{(a,pd)=1} (1 - t^{ak})^{a^{p-3}\chi(a)}.$$

Then

$$(\kappa_1)_{\omega^2\chi} \text{ is a } p\text{-th power mod } \lambda \Leftrightarrow Q^{kd} \equiv 1 \bmod l.$$

Proof. See prop. 2.3.

Note

$$((\kappa_1)_{\omega^2\chi})^{\phi(pd)/2} = \prod_{(a,pd)=1} (1-\zeta_{pd}^a)^{\omega^2\chi(\sigma_a-1)}$$
$$\equiv \prod_{(a,pd)=1} (1-\zeta_{pd}^a)^{a^{p-3}\chi(a)} \bmod E^p.$$

Define

$$Z := \prod_{(a,pd)=1} (1-\zeta_{pd}^a)^{a^{p-3}\chi(a)} \bmod E^p.$$

Then $Z \equiv Q \bmod \lambda$.
Furthermore,

$$Z \text{ is a } p\text{-th power } \Leftrightarrow (\kappa_1)_{\omega^2\chi} \text{ is a } p\text{-th power.}$$

After sorting out all the cases where $(A)_{\omega^2\chi}$ is trivial, there are 5 cases left. For those I cannot find a prime such that $(\kappa_1)_{\omega^2\chi}$ is not a p-th power of a unit in L^+. This would mean that $\#(E^+_{L_M}/C^+_{L_M})_{\omega^2\chi}$ is not trivial, but I am unable to prove it. For these 5 cases the following lemma will be applied which can be found in chapter 1.

Lemma 3.8 *Let $M = p(\#(A)_{\omega^{-1}\chi})^2$ and $d = p$ disc (F). Then*

$A_{\omega^{-1}\chi}$ is cyclic $\Leftrightarrow$ there is a prime $q \equiv 1$ mod dM such that $d(q) = 1$.

For $q \equiv 1$ mod d^2M we have

$$d(q)\mathbf{Z}/M\mathbf{Z} = (\sum_{a\in(\mathbf{Z}/d\mathbf{Z})^*} \nu_q(-1/(at)!)\omega\chi(a))\mathbf{Z}/M\mathbf{Z}.$$

We have to prove that there exists a prime $q \equiv 1 \bmod d^2M$ such that

$$p \nmid \sum_{a\in(\mathbf{Z}/d\mathbf{Z})^*} \nu_q(-1/(at)!)\chi(a)a.$$

Those primes q are very large. For example, for $(7741, 7)$ we have to try the prime 1085683145711627. So this is not a realistic method, unless the term $\nu_q(-1/(at)!)$ can be simpified or M can be chosen smaller.

This gives the following unsolved cases:

$$\begin{array}{ll} (7741,7) & (10088,7) \\ (13465,7) & (17160,7) \\ (13521,17) & \end{array}$$

We still have the cases where $p \mid$ disc (F). It will turn out that we can apply all the methods described above, as long as $p \neq 5$ and $F \neq \mathbf{Q}(\sqrt{p})$ for $p \equiv 1 \bmod 4$.

3.6.1 $p \mid$ disc (F)

Let d be equal to disc (F), take $L = \mathbf{Q}(\zeta_d)$, and $K = F(\zeta_p)$.
Since $e_p(F) = 2$ we have in the exact sequence of theorem 3.7 that S' is empty, which implies

$$(\mu_p \otimes Cl(O_K[\tfrac{1}{p}]))^\Gamma \cong K_2(O_F)/p.$$

Also

$$(A/A^p)_{\omega^{-1}} \cong (\mu_p \otimes Cl(O_K))^\Gamma,$$

and

$$(\mu_p \otimes Cl(O_K))^\Gamma \twoheadrightarrow (\mu_p \otimes Cl(O_K[\frac{1}{p}]))^\Gamma.$$

To be able to apply the described methods we need:

i). $\mathrm{Gal}(K/\mathbf{Q}) \cong \mathrm{Gal}(F/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$,

ii). $\omega^{-1}\chi$ is a primitive character of conductor pd,

iii). $\omega^2\chi$ is a primitive character of conductor pd.

The first condition is satisfied as long as $F \neq \mathbf{Q}(\sqrt{p})$ for $p \equiv 1 \bmod 4$.

The second condition is satisfied for all fields $F \neq \mathbf{Q}(\sqrt{p})$ for $p \equiv 1 \bmod 4$. This can be seen as follows:
The order of $\omega^{-1}\chi$ is $p-1$, so it is a primitive character of a subfield of degree $p-1$ over $\mathbf{Q}$ or of K itself. The only field in which the conductor would be less than pd is $\mathbf{Q}(\zeta_p)$. This can only be the case if $F = \mathbf{Q}(\sqrt{p})$, for $p \equiv 1 \bmod 4$.

The third condition is satisfied as long as $p \neq 5$ and $F \neq \mathbf{Q}(\sqrt{p})$ for $p \equiv 1 \bmod 4$. We have that $\omega^2\chi$ corresponds at least to an extension of degree $\operatorname{lcm}(\frac{p-1}{2}), 2)$ over $\mathbf{Q}$. If $p \equiv 3 \bmod 4$ proceed in the same way as in (ii). For $p \equiv 1 \bmod 4$, the only extension which would force the conductor to be less than d is $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ for $p > 5$. This can only be the case if $F = \mathbf{Q}(\sqrt{p})$, for $p \equiv 1 \bmod 4$.
For $p = 5$ the corresponding field is a quadratic subfield in which the conductor is less than pd. For example, if χ is the character corresponding to $\mathbf{Q}(\sqrt{15})$ and ω^2 the character corresponding to $\mathbf{Q}(\sqrt{5})$, then $\omega^2\chi$ is the character corresponding to $\mathbf{Q}(\sqrt{3})$.

For $p \mid \text{disc}\,(F)$ there is only one unsolved case namely (7945,7).

Putting everything together we get the following list of unsolved cases for disc (F) less than 20000:

(11861,7)	(6497,11)	(18921,13)
(7741,7)	(10088,7)	(13465,7)
(17160,7)	(13521,17)	(7945,7)

For all the other cases we have that the p-Sylow subgroup of the tame kernel is cyclic.

Remark 3.2 If the p-sylow subgroup of the tame kernel is always cyclic, then $A_{\omega^{-1}\chi}$ is always cyclic. This implies using the reflection principle that $(E_M^+/C_M^+)_{\omega^2\chi} \cong A_{\omega^2\chi}$.

3.6.2 A possible counter example for $p = 5$

Browkin pointed out to me that in [Mes] it has been proven using the theory of elliptic curves that there are infinitely many real and imaginary quadratic fields whose 5-rank of the ideal class group equals or is larger than 3. Mestre constructs a field $K = \mathbf{Q}(y)$, where y is given by the elliptic curve

$$y^2 = 42(44876601x - 133597561)(9261x^2 - 6061).$$

In this equation x is defined by

$$x = \frac{c_4z^4 + c_3z^3 + c_2z^2 + c_1z + c_0}{5167944494559(4883562662z + 922989409)(11z - 29)z}.$$

Here $c_0 = 343898806423252015354080$,
$c_1 = -411804539876837130626339$,
$c_2 = -642297925780193483509181$,
$c_3 = 826467660375890872281118$, and
$c_4 = 138516062261536496425152 0$.

In order to obtain that the 5-rank of K is larger than or equal to 3, the following conditions on z are given:

$z \equiv 0 \bmod 11 \cdot 19 \cdot 29$, $z \not\equiv \pm 86 \bmod 419$ and $z \equiv 1 \bmod 163 \cdot 701 \cdot 1277$.

Theorem 5.5 of [B] says that the 5-rank of the tame kernel of a real quadratic number field $\mathbf{Q}(\sqrt{d})$ is larger than or equal to the 5-rank of the ideal class group of $\mathbf{Q}(\sqrt{5d})$. So we need to find a z satisfying the above conditions and such that $5 \mid y$.
A possible z would be $163 \cdot 701 \cdot 1277 \cdot (5993 + 6061 \cdot 4) + 1$. Then $z \bmod (11 \cdot 19 \cdot 29) = 0$ and $z \bmod 419$ is not equal to ± 86. Thus the 5-rank of $K = \mathbf{Q}(y)$ is equal to or larger than 3.

Here $y = (97244314772274647562187733143557148978613690832088190$
$836849966029176010730887528816251111666189796809660591977966 70$
$828017498518097900874814478881205633867339309381549635403231 99$
$755513365198118349799258289167112526713429102797918195140398 11$
$882033777732066219531762880951300287907159852732567 05)^{1/2}$.

So $d = 19448862954454929512437546628711429795722738166417638 16$
$736999320583520214617750576325022233323795936193211839559334 16$
$560349970361958017496289577624112677346786187630992708064639 95$
$110267303962366995985165783342250534268582055958363902807962 37$
$640675554641324390635257619026005758143197054651341$.

This gives that the 5-rank of the tame kernel of $K_2\mathbf{Q}(\sqrt{d})$ is not cyclic, with d as above. This is a possible counter example, because 5 may divide $\phi(\text{ cond } \mathbf{Q}(d))$. For the smaller primes in the prime factorization 5 does not divide $\phi(\text{ cond } \mathbf{Q}(d))$. For the bigger primes in the prime factorisation I do not know this.

In the same way as is done for a real quadratic number field, we can look at the tame kernel of an imaginary quadratic number field. I will briefly discuss this.

3.7 The tame kernel of an imaginary quadratic number field

Fix a prime p as before and let F be imaginary quadratic. As we have seen $\#(A)_{\omega^{-1}\times 1} = 1$ for $p \geq 5$. So $\#(A)_{\omega^{-1}} = \#(A)_{\omega^{-1}\chi}$.

If $L = \mathbf{Q}(\zeta_{pd})$ with $d = \mid \text{disc}(F) \mid$, then

$(\kappa_1)_{\omega^{-1}\chi}$ is a p-th power of a unit in $L^+ \Leftrightarrow K_2(O_F)\{p\}$ non trivial.

A faster way to obtain results, is to use the reflection principle first and then to look at the units.

Recall $0 \leq a_{\omega^2\chi^{-1}} - a_{\omega^{-1}\chi} \leq 1$. We know

$$\#(A)_{\omega^2\chi} = p^{\mathrm{ord}_p B_{1,\omega^{-2}\chi}}.$$

So if $p \mid B_{1,\omega^{-2}\chi}$, $p^2 \nmid B_{1,\omega^{-2}\chi}$ then $(A)_{\omega^2\chi}$ is cyclic, which implies that $K_2O_F\{p\}$ is cyclic or trivial.
In the same way as before $p^2 \nmid B_{1,\omega^{-2}\chi}$ is equivalent with

$$p^3 \nmid \sum_{a=1,(a,pd_F)=1}^{p|d_F|} a^{p^2(p-3)+1}\left(\frac{d_F}{a}\right).$$

For the cases where the structure is still not clear, determine if $(\kappa_1)_{\omega^{-1}\chi}$ is a p-th power of a unit in L^+.

Remark 3.3 For $p \mid$ disc (F) everything works as long as $F \neq \mathbf{Q}(\sqrt{p})$ for $p \equiv 3 \bmod 4$ and $p \neq 5$.

In the next section a list of the size of $K_2\mathbf{Z}[\zeta_n + \zeta_n^{-1}]$ for $n \leq 100$ will be given and ranks will be computed.

3.8 The tame kernel of the maximal real subfield of a cyclotomic field

In the first column we have $K_2\mathbf{Z}[\zeta_n + \zeta_n^{-1}]$, in the second column the prime factorization of the number of elements of $K_2\mathbf{Z}[\zeta_n + \zeta_n^{-1}]$ and in the third column the ranks.

The structure of the Abelian group $K_2\mathbf{Z}[\zeta_n + \zeta_n^{-1}]$

3	2	rk_2=1
5	2^2	rk_2=2
7	2^3	rk_2=3
8	2^2	rk_2=2
9	2^3	rk_2=3
11	$2^5, 5$	rk_2=5
12	2^2	rk_2=2
13	$2^6, 19$	rk_2=6
15	2^5	rk_2=4, rk_4=1
16	$2^4, 5$	rk_2=4
?17	$2^{11}, 73$	rk_2=9
?19	$2^9, 3^2, 487$	rk_2=9
20	$2^4, 5$	rk_2=4
21	$2^7, 7$	rk_2=6, rk_4=1
23	$2^{11}, 11, 37181$	rk_2=11
24	$2^4, 3$	rk_2=4
25	$2^{10}, 71, 641$	rk_2=10
27	$2^9, 19, 307$	rk_2=9
28	$2^8, 13$	rk_2=6, rk_8=1
?29	$2^{20}, 3, 7, 43, 17837$	rk_2=14
?31	$2^{17}, 5^2, 7, 11, 2302381$	rk_2=17
32	$2^8, 3^2, 5, 97$	rk_2=8, rk_3=2
33	$2^{11}, 3, 5, 421$	rk_2=11
35	$2^{13}, 13^2, 37, 61$	rk_2=12, rk_4=1, rk_{13}=2
36	$2^6, 31$	rk_2=6
?37	$2^{18}, 3^2, 5, 7, 19, 37, 73,$ $577, 17209$	rk_2=18
?39	$2^{14}, 3^4, 13^2, 19$	rk_2=12, rk_3=2, rk_{13}=1

40	$2^8, 5, 7, 41$	$rk_2=8$
?41	$2^{24}, 5, 13, 31^2, 431,$ 250183721	$rk_2=21, rk_8=1, rk_{31}=1$
?43	$2^{23}, 7, 19, 29, 463, 1051,$ 416532733	$rk_2=21$
44	$2^{10}, 5, 7, 31, 101$	$rk_2=10$
45	$2^{13}, 73, 3637$	$rk_2=12, rk_4=1$
47	$2^{23}, 23, 139, 82397087,$ 12451196833	$rk_2=23$
48	$2^8, 3, 5, 73$	$rk_2=8$
49	$2^{21}, 113, 2437, 1940454849859$	$rk_2=21$
?51	$2^{21}, 73, 13004081$	$rk_2=17$
52	$2^{12}, 13, 19, 73, 769$	$rk_2=12$
53	$2^{26}, 7, 13, 85411, 96331,$ $379549, 641949283$	$rk_2=26$
?55	$2^{22}, 5^4, 11^2, 41, 5581, 16061$	$rk_2=20, rk_5=2, rk_{11}=2$
?56	$2^{15}, 3, 5, 11^2, 13, 43$	$rk_2=12, rk_{11}=2$
?57	$2^{19}, 3^2, 7, 19, 97, 487, 83701$	$rk_2=19$
59	$2^{29}, 29, 59,$ $998855361369139381235879427 1$	$rk_2=29$
60	$2^{11}, 3, 5$	$rk_2=8, rk_{16}=1$
61	$2^{30}, 5, 7^2, 11^2, 19, 31, 2081, 2801,$ $40231, 411241, 514216621$	$rk_2=30, rk_7=2, rk_{11}=2$
?63	$2^{23}, 5^2, 7^2, 19, 67, 193, 211$	$rk_2=18, rk_5=2, rk_7=2$
64	$2^{16}, 3^2, 5, 17, 97, 93377873$	$rk_2=16, rk_3=2$
?65	$2^{41}, 7^2, 19, 29, 37^2, 61, 97, 107^2$	$rk_2=27, rk_7=2$ $rk_{37}=2, rk_{107}=2$
67	$2^{33}, 11, 67, 193, 661^2, 2861,$ $8009, 11287, 9383200455691459$	$rk_2=33, rk_{661}=2$
?68	$2^{20}, 17, 73, 48741313$	$rk_2=17$

69	$2^{24}, 3, 11, 23, 37181, 21796416731$	$rk_2=22, rk_8=1$
71	$2^{35}, 5, 7, 31, 113, 211, 281, 701^2,$	$rk_2=35, rk_{701}=2$
	$12713, 13070849919225655729061$	
72	$2^{12}, 3^2, 13, 19, 31, 79$	$rk_2=12, rk_3=1$
?73	$2^{39}, 3^2, 11, 79, 89, 241, 23917,$	$rk_2=39$
	$3341773, 11596933,$	
	31964959893317833	
75	$2^{21}, 71, 641, 5797259381$	$rk_2=20$
?76	$2^{18}, 3^2, 19, 109, 229, 487, 221203$	$rk_2=18$
?77	$2^{44}, 3^2, 5, 11, 19^2, 31, 139, 181,$	$rk_2=30, rk_{19}=2$
	$3855211, 19916791$	
79	$2^{39}, 13, 157, 199, 521^2, 1249,$	$rk_2=39, rk_{521}=2$
	$4447, 323623, 1130429,$	
	68438648614508149381	
80	$2^{16}, 5^2, 7, 41, 269, 337, 409$	$rk_2=16, rk_5=2$
81	$2^{27}, 19, 307, 571010149,$	$rk_2=27$
	325982579770423	
83	$2^{41}, 41, 17210653, 151251379,$	$rk_2=41$
	$18934761332741,$	
	48833370476331324749419	
84	$2^{15}, 7, 13, 397$	$rk_2=12, rk_{16}=1$
?85	$2^{45}, 3^2, 5, 17, 73, 137, 257, 1201,$	$rk_2=35, rk_3=1$
	$1697, 3678977, 4760689$	
?87	$2^{38}, 3, 7, 13, 17, 43, 17837,$	$rk_2=28$
	677266776095561	
88	$2^{20}, 5, 7, 11^2, 23, 31^2, 101,$	$rk_2=20, rk_{11}=2, rk_{31}=2$
	$641, 15641$	
89	$2^{47}, 5, 11, 13, 37, 397, 4027,$	$rk_2=47$
	$262504573, 15354699728897,$	
	$49135060828995551670374357$	

?91	$2^{47}, 3^2, 5, 7, 13, 19, 37, 61, 73, 109$ $139, 151, 241, 673,$ $5881, 64153, 304069$	rk_2=36
92	$2^{24}, 5, 11, 463, 9857,$ $37181, 7578143$	rk_2=22, rk_8=1
?93	$2^{37}, 3^3, 5^2, 7^2, 11, 19^2,$ $31, 274831, 2302381, 11822821$	rk_2=30, rk_3=1, rk_7=2 rk_{19}=2
?95	$2^{39}, 3^4, 5, 13^3, 19, 37, 61, 421, 487,$ $7507, 7741, 14221, 50483076769$	rk_2=36, rk_{13}=3
96	$2^{16}, 3^3, 5, 73, 97, 324889$	rk_2=16, rk_3=3
?97	$2^{52}, 5^2, 7^2, 17, 149, 241, 367,$ $421, 2753, 147689, 651997,$ $21205889, 41481169, 5429704177,$ 2758053952369	rk_2=49, rk_5=2, rk_7=2
99	$2^{31}, 3^2, 5, 13^2, 31^2, 421^2,$ $51001, 510481, 3646681$	rk_2=31, rk_3=1, rk_{13}=1, rk_{31}=2, rk_{421}=2
100	$2^{20}, 5^2, 71, 641, 34732500521$	rk_2=20, rk_5=1

3.8.1 Computational remarks

The number of elements of the tame kernel have been computed using theorem 3.5 and lemma 3.4. The number of elements for $n = 83, 89, 97$ were sent to me by Browkin, who on his turn received tables from Hettling of $w_2(F)\zeta_F(-1)$ for all subfields F of the maximal real subfield of $\mathbf{Q}(\zeta_n)$ where $n \leq 100$.

A "?" denotes that I do not know the structure completely. The size of the class numbers used in the sequel can be found in [W].

If p is an odd prime such that a power of p divides the number of elements and p does not divide $n\phi(n)$, we can proceed as before using

the isomorphism

$$K_2(O_F)/p \cong (A/A^p)_{\omega^{-1}}.$$

For some cases the rank follows directly from:

$$B_{1,\omega\chi} \equiv \frac{B_{2,\chi}}{2} \bmod p.$$

For the other cases we will compute $B_{1,\omega\chi}$ for several χ. Note that it is not necessary to compute all the Bernoulli numbers. This follows from: $\mathrm{Gal}(\mathbf{Q}_p(\zeta_{\phi(n)})/\mathbf{Q}_p)$ is generated by the Frobenius automorphism σ which sends $\zeta \to \zeta^p$. In lemma 2.2 it is proved that σ permutes the linear characters that occur in the decomposition of an irreducible $\mathbf{Z}_p$ representation, and that the corresponding eigenspaces are isomorphic. In other words, the p-valuations of the corresponding Bernoulli numbers are equal. So in most cases it will be sufficient to look at the characters with values in $\mathbf{Q}_p$. The following example illustrates this.

Example 3.1 For $n = 41$ we have that 31^2 divides the number of elements. If τ is an even character of $\mathrm{Gal}(\mathbf{Q}(\zeta_{41})/\mathbf{Q})$ then the values of $\omega\tau^{-1}$ belong to $\mathbf{Q}_{31}(\zeta_{20})$. Since $\mathbf{Q}_{31}(\zeta_{20})/\mathbf{Q}_{31}$ is an extension of degree 2, we obtain that the following characters occur in pairs: $(\tau, \tau^{11}), (\tau^3, \tau^{13}), (\tau^5, \tau^{15}), (\tau^7, \tau^{17})$ (τ^9, τ^{19}).
So if 31 does not divide one of the remaining Bernoulli numbers then the 31-rank of the tame kernel is 2. In this case 31 did divide only one of them and 31^2 did not, so the 31-rank of $K_2[\mathbf{Z}\zeta_{41} + \zeta_{41}^{-1}]$ equals 1.

Using

$$(A/(A^p))_{\omega^{-1}} \cong \bigoplus_{\chi \in \widehat{\mathrm{Gal}(F/\mathbf{Q})}} (A/(A^p))_{\omega^{-1}\chi},$$

we see that the p-rank of the tame kernel is built by the p-ranks of the tame kernels of the cyclotomic subfields.

As an example consider $n = 64$. Here we have that 3^2 divides the number of elements. For $n = 32$ we have that the 3-rank equals 2. Thus for [64] the 3-rank must be equal to 2.

This can also be derived using the following lemma.

Lemma 3.9 *Let E/F be a Galois extension with group Γ. Let S be a set of primes of F containing the infinite primes, and let T consist of the primes of E above the primes in S. Then*

$$K_2(O_{F,S})/n \cong (K_2(O_{E,T})/n)^{\Gamma}$$

is an isomorphism if n and $|\Gamma|$ are relative prime.

Proof. See [K].
This lemma can also be used for the prime $p = 2$.

Example 3.2 For $n = 69$ we have that 2^{24} divides the number of elements, where the 2-rank is equal to 22.
Browkin computed that the 8-rank of $K_2(O_{\mathbf{Q}(\sqrt{69})}) = 1$.
If we take $F = \mathbf{Q}(\sqrt{69})$ and $E = \mathbf{Q}(\zeta_{69} + \zeta_{69}^{-1})$, it follows that the 8-rank of [69] is 1.

For the 2-rank of the tame kernel we have used the following formula from Keune (see [K]), where O_F denotes the ring of integers of a number field F,

$$\mathrm{rk}_2(K_2O_F) = \mathrm{rk}_2Cl(O_F[\tfrac{1}{2}]) + r_2 + r - 1.$$

Here r_2 denotes the number of primes of F above 2 and r is the number of real infinite primes of F.

If p is odd and divides $n\phi(n)$ we have to use theorems 3.6, 3.7 and the following exact sequence which can be derived from theorem 3.6 (See theorem 6.6 of [K]).
Let p be an odd prime, or $p = 2$ and F contains i or $\sqrt{-2}$. Write Γ for $\mathrm{Gal}(F(\zeta_{p^r})/F)$ and let Z_p denote the decomposition group of $\mathfrak{p}$ in $F(\zeta_{p^r})/F$, then

$$0 \to (\mu_{p^r} \otimes Cl(O_{F(\zeta_{p^r})}[\tfrac{1}{p}]))_{\Gamma} \to K_2^+(O_F)/p^r \to \bigoplus_{\mathfrak{p}|p} (\mu_{p^r})_{Z_p} \to (\mu_{p^r})_{\Gamma} \to 0.$$

Proof. Let S be the set of primes of F containing the infinite primes and the finite primes $\mathfrak{p}$ for which $N(\mathfrak{p})-1$ and the ramification index $e_{\mathfrak{p}}$ of $\mathfrak{p}$ in $F(\zeta_{p^r})/F$ are not relative prime and let T denote the primes of $F(\zeta_{p^r})$ above S. Then

$$(K_2^+(O_{F(\zeta_{p^r}),T}))_\Gamma \cong K_2^+(O_{F,S}).$$

Let $\mathfrak{q}$ denote the prime of $F(\zeta_{p^r})$ above p. Write $(\bigoplus_{\mathfrak{q}|p}\mu_{p^r})_0$ for the kernel of

$$\bigoplus_{\mathfrak{q}|p}\mu_{p^r} \to \mu_{p^r},$$

then $(\bigoplus_{\mathfrak{q}|p}\mu_{p^r})_0$ is a cohomologically trivial Γ-module. For proofs of the assertions see [K].

From now on suppose p is odd.
If $p \mid n$ with $F = \mathbf{Q}(\zeta_n + \zeta_n^{-1})$, then $\Gamma = \mathrm{Gal}(F(\zeta_p)/F) \cong \mathbf{Z}/2$ and

$$(\mu_p \otimes Cl(O_{F(\zeta_p)}))^\Gamma \cong (A/(A^p))^-.$$

Moreover, if p does not divide the class number of $\mathbf{Q}(\zeta_m)$, with $n = pm$, $(p,m) = 1$, then

$$Cl(O_{F(\zeta_p)}) \cong Cl(O_{F(\zeta_p)}[\tfrac{1}{p}]),$$

since the primes above p do not generate the p-part of $Cl(\mathbf{Q}(\zeta_m))$ and ramify completely afterwards.

Example 3.3 For $n = 63$, we have that 7^2 divides the number of elements. 7 does not divide the class number of $\mathbf{Q}(\zeta_9)$, so the primes above 7 are not generators for the 7-part of the ideal class group of $\mathbf{Q}(\zeta_{63})$. If we use theorem 3.7 we get an exact sequence

$$0 \to \mathbf{Z}/7 \to K_2(O_F)/7 \to \mu_7 \to 0,$$

so the 7-rank of [63] equals 2.

If a power of p divides the minus class number then the structure of the class group is needed in most cases. Sometimes this can be derived by using knowledge of the tame kernel of subfields.

Example 3.4 The minus ideal class group of $\mathbf{Q}(\zeta_{96})$ is isomorphic to $\mathbf{Z}/3 \times \mathbf{Z}/3$. This can be derived as follows: 3^3 divides the number of elements of [96]. We know that the 3-rank of [32] is equal to 2, and

$$K_2 O_{\mathbf{Q}(\zeta_{32}+\zeta_{32}^{-1})}/3 \cong (\mu_3 \otimes (Cl(O_{\mathbf{Q}(\zeta_{32}+\zeta_{32}^{-1})(\zeta_3)}))^{\Gamma},$$

since 3 does not divide the class number of $\mathbf{Q}(\zeta_{32})$.
The norm maps the ideal class group of $\mathbf{Q}(\zeta_{96})$ onto the ideal class group of $\mathbf{Q}(\zeta_{32}+\zeta_{32}^{-1})(\zeta_3)$. We conclude that the minus ideal class group of $\mathbf{Q}(\zeta_{96})$ is isomorphic to $\mathbf{Z}/3 \times \mathbf{Z}/3$ and the 3-rank of [96] is equal to 3.

If a power of p, say p^r, divides n and p splits between F and $F(\zeta_p)$, then we have a surjection

$$K_2^+(O_F)/p^r \to \bigoplus_{\mathfrak{p}|p} \mu_{p^r} \to 0,$$

since $Z_p = 1$.

As an example take $F = \mathbf{Q}(\zeta_{99}+\zeta_{99}^{-1})$, then 3^2 divides the number of elements of [99]. So the 3-rank equals 1.

Suppose $2^r \mid n$, with $r \geq 2$. Then in some cases we can deduce from theorem 3.6 the structure of $K_2^+ O_E$ where $E = \mathbf{Q}(\zeta_n)$ and this gives using the isomorphism

$$(K_2^+(O_{F(\zeta_{p^r}),T}))_{\Gamma} \cong K_2^+(O_{F,S}),$$

and the exact sequence

$$0 \to K_2^+(O_F) \to K_2(O_F) \to \bigoplus_{p \text{ real infinite}} \mu_2 \to 0$$

in some cases the structure of the 2-part.

Example 3.5 If $E = \mathbf{Q}(\zeta_{60})$ then the 2-part of the ideal class group of E is trivial. This gives $K_2^+ O_E/4 \cong \mathbf{Z}/4$. Write F for the maximal real subfield then, $K_2^+ O_F$ is also a cyclic group. We know $\mathrm{rk}_2 K_2 O_F = 8$. Put all this in the exact sequence above to obtain

$$(K_2(O_F))_2 = \mathbf{Z}/16 \bigoplus_{7\times} \mathbf{Z}/2.$$

Bibliography

[B] J. Browkin, On the p-rank of the tame kernel of algebraic number fields, *J. reine angew. Math.* **432** (1992), 135–149.

[C-R] C.W. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras*, Wiley (1962).

[G] M. Geijsberts, *The tame kernel, computational aspects*, thesis, Nijmegen (1991).

[Ga] H. Garland, A finiteness theorem for K_2 of a number field, *Ann. of Math.* **94** (1971), 534–548.

[Gr] C. Greither, Class groups of Abelian fields and the main conjecture, *Ann. Inst. Fourier* **42**, 3 (1992), 449–499.

[I] I. M. Isaacs, *Character theory of finite groups*, Academic Press (1976).

[K] F. Keune, On the structure of the K_2 of the ring of integers in a number field, *K-Theory* **2** (1989), 625–645.

[Ko] V. A. Kolyvagin, Euler Systems, in: *The Grothendieck Festschrift vol. II*, Progr. Math. 87 (1990), 435–483.

[L-M] R.C. Laubenbacher, B.A. Magurn, SK_2 and K_3 of dihedral groups, *Can. J. Math.* **44** (1992), 591–623.

[La1] S. Lang, *Algebraic number theory*, Grad. Texts in Math. 110, Springer-Verlag (1986).

[La2] S. Lang, *Cyclotomic fields*, Grad. Texts in Math. 59, Springer-Verlag (1978).

[M-W] B. Mazur, A. Wiles, Class fields of Abelian extensions of $\mathbf{Q}$, *Invent. Math.* **76** (1984), 179–330.

[Mes] J.-F. Mestre, Corps quadratiques dont le 5-rang du groupe des classes est ≥ 3, *C.R. Acad. Sc. Paris*, **315**, (1992), 371–374.

[Me-S] A.S. Merkurjev, A.A. Suslin, *On the K_3 of a field*, LOMI preprint E-2-87, (1987).

[Mi] J. Milnor, *Introduction to algebraic K-theory*, Annals of Math. Studies 72, Princeton Univ. Press (1971).

[Ru1] K. Rubin, The main conjecture, appendix to: *Cyclotomic fields I and II*, S. Lang, Grad. Texts in Math. 121, Springer-Verlag (1990), 379–419.

[Ru2] K. Rubin, Kolyvagin's system of Gauss sums, in: *Arithmetic algebraic geometry*, Birkhauser (1991), 309–324.

[Ru3] K. Rubin, Stark units and Kolyvagin's "Euler systems", *J. reine angew. Math.* **425** (1992), 141–154.

[Ru4] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* **103** (1991), 25–68.

[Se] J.- P. Serre, *Local fields*, Grad. Texts in Math. 67, Springer-Verlag (1979).

[Si1] W. Sinnott, On the Stickelberger ideal and the circular units of a cyclotomic field, *Ann. of Math.* (2), **108** (1978), 107–134.

[Si2] W. Sinnott, On the Stickelberger ideal and the circular units of an Abelian field, *Invent. Math.* **62** (1980), 181–234.

[Ta] J. Tate, Relations between K_2 and Galois Cohomology, *Invent. Math.* **36** (1976), 257–274.

[W] L. C. Washington, *Introduction to cyclotomic fields*, Grad. Texts in Math. 83, Springer-Verlag (1982).

[Wi] A. Wiles, The Iwasawa conjecture for totally real fields, *Ann. of Math.* **131**, 493–540 (1990).

Samenvatting

Dit proefschrift bestaat uit 3 hoofdstukken. De verbindende schakel tussen deze 3 hoofdstukken is het isomorfisme

$$(Cl(O_{F(\zeta_p)})/p)_{\omega^{-1}} \cong K_2O_F/p.$$

Hierbij is F een Abels getallenlichaam, en p een priem die onvertakt is in F en $[F : \mathbf{Q}]$ niet deelt. Voor het bewijs van dit isomorfisme is de exacte rij

$$0 \to (\mu_p \otimes Cl(O_{F(\zeta_p)}[\tfrac{1}{p}]))^\Gamma \to K_2O_F/p \to \bigoplus_{p \in S'} \mu_p \to 0$$

van Keune ([K]) nodig.

In hoofdstuk 1 en 2 wordt de linkerkant van het isomorfisme bekeken. Hiervoor wordt

$$(O \otimes_{\mathbf{Z}_p} Cl(O_{F(\zeta_p)})/p)_{\omega^{-1}}$$

geschreven als

$$(\bigoplus_{\chi \text{ odd}} (O \otimes_{\mathbf{Z}_p} Cl(O_{F(\zeta_p)})/p)_{\omega^{-1}\chi}) \bigoplus (\bigoplus_{\chi \text{ even}} (O \otimes_{\mathbf{Z}_p} Cl(O_{F(\zeta_p)})/p)_{\omega^{-1}\chi}).$$

In hoofdstuk 1 is het aantal elementen van het oneven gedeelte uitgedrukt in Bernoulli getallen.
Vervolgens is in hoofdstuk 2 het aantal elementen van het even gedeelte uitgedrukt in het aantal elementen van eigenruimten van de globale eenheden modulo de cyclotomische eenheden.
In hoofdstuk 3 zijn de verkregen resultaten van de hoofdtukken 1 en 2 toegepast op de rechterkant van het isomorfisme om iets over de structuur van de tamme kern te zeggen.

Dankwoord

Op deze plaats wil ik iedereen bedanken die heeft bijgedragen aan het tot stand komen van dit proefschrift. Frans Keune wil ik bedanken voor de mogelijkheid om dit proefschrift te schrijven, voor de talloze onderwerpen die hij in het begin heeft aangedragen en vooral voor het op weg helpen met hoofdstuk 2. Engelbert, Ben, Willy en vooral Floris wil ik bedanken voor de tijd die zij in LaTeX hebben gestoken en andere aanverwante computer zaken. I would like to thank Jerzy Browkin for sending me his list with unknown structures, and for the remarks on my thesis. Tot slot wil ik nog mijn vrienden en familie bedanken, die altijd bereid waren te luisteren. Als allerlaatste bedank ik Arno voor alles wat hij voor me heeft gedaan.

Curriculum Vitae

De schrijfster van dit proefschrift is geboren op 17 december 1966 in Amsterdam. In 1986 ging ze wiskunde studeren aan de Universiteit van Amsterdam. In 1991 behaalde ze haar doctoraalexamen, waarna zij in 1992 AIO werd aan de Katholieke Universiteit van Nijmegen. Momenteel is zij werkzaam bij het Centraal Bureau voor de Statistiek.